State of Maine
Master Score Sheet

RFP# 202401005					
Improve Delivery of Digital Services to Constituents					
Bidder Name:		**Active Cyber**	**Carahsoft**	**Deloitte**	**Microsoft**
Proposed Cost:		**$32,091,320.00**	**$22,521,533.82**	**$34,935,517.34**	**$20,017,462.34**
Scoring Sections	**Points Available**				
Section I: Preliminary Information	N/A	N/A	N/A	N/A	N/A
Section II: Organization Qualifications and Experience	25	3	5	1	11
Section III: Proposed Services	50	17	10	40	27
Section IV: Cost Proposal	25	15.59	22.22	14.32	25
TOTAL	**100**	**35.59**	**37.22**	**55.32**	**63**
Bidder Name:		**PruTech**	**Servos**	**Maine Information Network, LLC dba Tyler Maine**	
Proposed Cost:		**$51,176,746.78**	**$32,250,725.00**	**$27,289,817.00**	
Scoring Sections	**Points Available**				
Section I: Preliminary Information	N/A	N/A	N/A	N/A	
Section II: Organization Qualifications and Experience	25	23	2	22	
Section III: Proposed Services	50	19	8	35	
Section IV: Cost Proposal	25	9.78	15.52	18.34	
TOTAL	**100**	**51.78**	**25.52**	**75.34**	

REV 4/4/2023

Award Justification Statement
RFP# 202401005 Delivery of Digital Services to Constituents

- **Summary**

  The State of Maine, Department of Administrative and Financial Services, Information Technology is seeking to procure the technology, operation, maintenance, and support required to build the robust foundational blocks to create a Constituent-centric experience wherein Maine Constituents have the ability to interact with, manage, and receive State services seamlessly through a single source. The scope of services to be provided by the Bidder shall include hosting management, implementation, project management, training, support, marketing, governance, and maintenance. The awarded Bidder will be responsible for implementation, training, and all necessary professional services for the Constituents' Portal Platform Solution and the underlying technology to meet the requirements of the RFP.

- **Evaluation Process**

  An evaluation team of four individuals reviewed proposals submitted by bidders. A team of five subject matter experts evaluated the Technical Assessment portion and presented those findings to the evaluation team. Members of the proposal evaluation team completed individual reviews of each submitted proposal, then met as a team over three days to assign consensus scores for each proposal. The team evaluated one bidder at a time based on the criteria that was presented in the RFP. The qualifications and experience of evaluation team members encompassed the following areas of focus:
    - Security
    - Identity access management
    - Architecture
    - Project management
    - Data management
    - Web service technologies
    - Disclosure and consent management
    - Personalized notifications
    - Customer service

  After the initial scoring was complete, Tyler Maine, the highest scoring Bidder, was invited to demonstrate the proposed solution.

- **Qualifications & Experience**
    - Tyler Maine has provided online services to 550 Maine state and local partners since 1999.
    - Tyler Maine is part of Tyler Technologies which has 44,000 successful solution implementations across 13,000 locations in all 50 states.

- Tyler Maine possesses Maine domain expertise and existing legacy relationships with State of Maine agencies.
- Tyler Maine provided extensive past project examples that included thorough contact details as well as contact details for the subcontractor.
- Tyler Maine provided a meaningful, detailed organizational chart, thorough financials and $10 million coverage for cyber liability.

- **Proposed Services**
  - System security components
  - Identity proofing, lifecycle management
  - Multi-factor authentication
  - Data management
  - System requirements
  - Support requirements
  - Training and support
  - Disclosure and consent
  - Recommendation technology
  - Disaster recovery

- **Cost Proposal**
  The highest proposed cost was $51,176,746.78. The lowest proposed cost was $20,017,462.34. Tyler Maine's cost was $27,289,817.00.

- **Conclusion**
  Tyler Maine was the highest scoring Bidder. The proposal stood out due to the extensive provision of online services to numerous state of Maine entities. As part of a larger company, Tyler Maine demonstrates a robust capacity for delivering effective solutions. The company has significant domain experience and longstanding engagements with the state of Maine, further solidifying its credibility. Additionally, Tyler Maine provides extensive examples of past projects. Their proposed services are backed by strong, well-documented responses, making them a reliable choice for a conditional award.

STATE OF MAINE
DEPARTMENT OF Administrative
and Financial Services

Janet T. Mills
Governor

Kirsten Figueroa
Commissioner

AWARD NOTIFICATION LETTER

August 7, 2024

Active Cyber, LLC
Walter Lewis
5001 Spring Valley Rd, Suite 450E
Dallas, TX, 75244
Walter.lewis@activecyber.com

SUBJECT: Notice of Conditional Contract Award under RFP # 202401005, Improve Delivery of Digital Services to Constituents

Dear Walter:

This letter is in regard to the subject Request for Proposals (RFP), issued by the State of Maine Department of Administrative and Financial Services to Improve Delivery of Digital Services to Constituents. The Department has evaluated the proposals received using the evaluation criteria identified in the RFP, and the Department is hereby announcing its conditional contract award to the following bidder:

- Maine Information Network, LLC dba Tyler Maine

The bidder listed above received the evaluation team's highest ranking. The Department will be contacting the aforementioned bidder soon to negotiate a contract. As provided in the RFP, the Notice of Conditional Contract Award is subject to execution of a written contract and, as a result, this Notice does NOT constitute the formation of a contract between the Department and the apparent successful vendor. The vendor shall not acquire any legal or equitable rights relative to the contract services until a contract containing terms and conditions acceptable to the Department is executed. The Department further reserves the right to cancel this Notice of Conditional Contract Award at any time prior to the execution of a written contract.

As stated in the RFP, following announcement of this award decision, all submissions in response to the RFP are considered public records available for public inspection pursuant to the State of Maine Freedom of Access Act (FOAA). 1 M.R.S. §§ 401 et seq.; 5 M.R.S. § 1825-B (6).

This award decision is conditioned upon final approval by the State Procurement Review Committee and the successful negotiation of a contract. A Statement of Appeal Rights has been provided with this letter; see below.

Thank you for your interest in doing business with the State of Maine.

Sincerely,

Signed by:
Lisa Leahy
E43B9746D9D144A...

Lisa Leahy
Director of Digital Services
lisa.leahy@maine.gov

STATEMENT OF APPEAL RIGHTS

Any person aggrieved by an award decision may request an appeal hearing. The request must be made to the Director of the Bureau of General Services, in writing, within 15 days of notification of the contract award as provided in 5 M.R.S. § 1825-E (2) and the Rules of the Department of Administrative and Financial Services, Bureau of General Services, Division of Purchases, Chapter 120, § (2) (2).

STATE OF MAINE
DEPARTMENT OF Administrative
and Financial Services

Janet T. Mills
Governor

Kirsten Figueroa
Commissioner

AWARD NOTIFICATION LETTER

August 7, 2024

Carahsoft Technology Corporation
Matthew Sharer
11493 Sunset Hills Rd, Suite 100
Reston, VA, 20190
Matthew.sharer@carahsoft.com

SUBJECT: Notice of Conditional Contract Award under RFP # 202401005, Improve Delivery of Digital Services to Constituents

Dear Matthew:

This letter is in regard to the subject Request for Proposals (RFP), issued by the State of Maine Department of Administrative and Financial Services to Improve Delivery of Digital Services to Constituents. The Department has evaluated the proposals received using the evaluation criteria identified in the RFP, and the Department is hereby announcing its conditional contract award to the following bidder:

- Maine Information Network, LLC dba Tyler Maine

The bidder listed above received the evaluation team's highest ranking. The Department will be contacting the aforementioned bidder soon to negotiate a contract. As provided in the RFP, the Notice of Conditional Contract Award is subject to execution of a written contract and, as a result, this Notice does NOT constitute the formation of a contract between the Department and the apparent successful vendor. The vendor shall not acquire any legal or equitable rights relative to the contract services until a contract containing terms and conditions acceptable to the Department is executed. The Department further reserves the right to cancel this Notice of Conditional Contract Award at any time prior to the execution of a written contract.

As stated in the RFP, following announcement of this award decision, all submissions in response to the RFP are considered public records available for public inspection pursuant to

the State of Maine Freedom of Access Act (FOAA). 1 M.R.S. §§ 401 et seq.; 5 M.R.S. § 1825-B (6).

This award decision is conditioned upon final approval by the State Procurement Review Committee and the successful negotiation of a contract. A Statement of Appeal Rights has been provided with this letter; see below.

Thank you for your interest in doing business with the State of Maine.

Sincerely,

Signed by:
Lisa Leahy
E43B9746D9D144A...

Lisa Leahy
Director of Digital Services
lisa.leahy@maine.gov

STATEMENT OF APPEAL RIGHTS

Any person aggrieved by an award decision may request an appeal hearing. The request must be made to the Director of the Bureau of General Services, in writing, within 15 days of notification of the contract award as provided in 5 M.R.S. § 1825-E (2) and the Rules of the Department of Administrative and Financial Services, Bureau of General Services, Division of Purchases, Chapter 120, § (2) (2).

STATE OF MAINE
DEPARTMENT OF Administrative
and Financial Services

Janet T. Mills
Governor

Kirsten Figueroa
Commissioner

AWARD NOTIFICATION LETTER

August 7, 2024

Deloitte Consulting LLP
Scott Workman
30 Rockefellar Plaza, 41st floor
New York, NY, 10112
sworkman@delioitte.com

SUBJECT: Notice of Conditional Contract Award under RFP # 202401005, Improve Delivery of Digital Services to Constituents

Dear Scott:

This letter is in regard to the subject Request for Proposals (RFP), issued by the State of Maine Department of Administrative and Financial Services to Improve Delivery of Digital Services to Constituents. The Department has evaluated the proposals received using the evaluation criteria identified in the RFP, and the Department is hereby announcing its conditional contract award to the following bidder:

- Maine Information Network, LLC dba Tyler Maine

The bidder listed above received the evaluation team's highest ranking. The Department will be contacting the aforementioned bidder soon to negotiate a contract. As provided in the RFP, the Notice of Conditional Contract Award is subject to execution of a written contract and, as a result, this Notice does NOT constitute the formation of a contract between the Department and the apparent successful vendor. The vendor shall not acquire any legal or equitable rights relative to the contract services until a contract containing terms and conditions acceptable to the Department is executed. The Department further reserves the right to cancel this Notice of Conditional Contract Award at any time prior to the execution of a written contract.

As stated in the RFP, following announcement of this award decision, all submissions in response to the RFP are considered public records available for public inspection pursuant to

the State of Maine Freedom of Access Act (FOAA). 1 M.R.S. §§ 401 et seq.; 5 M.R.S. § 1825-B (6).

This award decision is conditioned upon final approval by the State Procurement Review Committee and the successful negotiation of a contract. A Statement of Appeal Rights has been provided with this letter; see below.

Thank you for your interest in doing business with the State of Maine.

Sincerely,

Signed by:
Lisa Leahy
E43B9746D9D144A...

Lisa Leahy
Director of Digital Services
lisa.leahy@maine.gov

STATEMENT OF APPEAL RIGHTS

Any person aggrieved by an award decision may request an appeal hearing. The request must be made to the Director of the Bureau of General Services, in writing, within 15 days of notification of the contract award as provided in 5 M.R.S. § 1825-E (2) and the Rules of the Department of Administrative and Financial Services, Bureau of General Services, Division of Purchases, Chapter 120, § (2) (2).

STATE OF MAINE
DEPARTMENT OF Administrative
and Financial Services

Janet T. Mills
Governor

Kirsten Figueroa
Commissioner

AWARD NOTIFICATION LETTER

August 7, 2024

Microsoft Corporation
Amanda Resten
1 Memorial Drive
Cambridge, MA 02142
amandaresten@microsoft.com

SUBJECT: Notice of Conditional Contract Award under RFP # 202401005, Improve Delivery of Digital Services to Constituents

Dear Amanda:

This letter is in regard to the subject Request for Proposals (RFP), issued by the State of Maine Department of Administrative and Financial Services to Improve Delivery of Digital Services to Constituents. The Department has evaluated the proposals received using the evaluation criteria identified in the RFP, and the Department is hereby announcing its conditional contract award to the following bidder:

- Maine Information Network, LLC dba Tyler Maine

The bidder listed above received the evaluation team's highest ranking. The Department will be contacting the aforementioned bidder soon to negotiate a contract. As provided in the RFP, the Notice of Conditional Contract Award is subject to execution of a written contract and, as a result, this Notice does NOT constitute the formation of a contract between the Department and the apparent successful vendor. The vendor shall not acquire any legal or equitable rights relative to the contract services until a contract containing terms and conditions acceptable to the Department is executed. The Department further reserves the right to cancel this Notice of Conditional Contract Award at any time prior to the execution of a written contract.

As stated in the RFP, following announcement of this award decision, all submissions in response to the RFP are considered public records available for public inspection pursuant to

the State of Maine Freedom of Access Act (FOAA). 1 M.R.S. §§ 401 et seq.; 5 M.R.S. § 1825-B (6).

This award decision is conditioned upon final approval by the State Procurement Review Committee and the successful negotiation of a contract. A Statement of Appeal Rights has been provided with this letter; see below.

Thank you for your interest in doing business with the State of Maine.

Sincerely,

Signed by:
Lisa Leahy
E43B9746D9D144A...

Lisa Leahy
Director of Digital Services
lisa.leahy@maine.gov

STATEMENT OF APPEAL RIGHTS

Any person aggrieved by an award decision may request an appeal hearing. The request must be made to the Director of the Bureau of General Services, in writing, within 15 days of notification of the contract award as provided in 5 M.R.S. § 1825-E (2) and the Rules of the Department of Administrative and Financial Services, Bureau of General Services, Division of Purchases, Chapter 120, § (2) (2).

STATE OF MAINE
DEPARTMENT OF Administrative
and Financial Services

Janet T. Mills
Governor

Kirsten Figueroa
Commissioner

AWARD NOTIFICATION LETTER

August 7, 2024

PruTech Solutions, Inc.
Will Brown
555 US Highway 1 South, Suite #230
Iselin, NJ, 08830
Proposals@prutech.com

SUBJECT: Notice of Conditional Contract Award under RFP # 202401005, Improve Delivery of Digital Services to Constituents

Dear Will:

This letter is in regard to the subject Request for Proposals (RFP), issued by the State of Maine Department of Administrative and Financial Services to Improve Delivery of Digital Services to Constituents. The Department has evaluated the proposals received using the evaluation criteria identified in the RFP, and the Department is hereby announcing its conditional contract award to the following bidder:

- Maine Information Network, LLC dba Tyler Maine

The bidder listed above received the evaluation team's highest ranking. The Department will be contacting the aforementioned bidder soon to negotiate a contract. As provided in the RFP, the Notice of Conditional Contract Award is subject to execution of a written contract and, as a result, this Notice does NOT constitute the formation of a contract between the Department and the apparent successful vendor. The vendor shall not acquire any legal or equitable rights relative to the contract services until a contract containing terms and conditions acceptable to the Department is executed. The Department further reserves the right to cancel this Notice of Conditional Contract Award at any time prior to the execution of a written contract.

As stated in the RFP, following announcement of this award decision, all submissions in response to the RFP are considered public records available for public inspection pursuant to

the State of Maine Freedom of Access Act (FOAA). 1 M.R.S. §§ 401 et seq.; 5 M.R.S. § 1825-B (6).

This award decision is conditioned upon final approval by the State Procurement Review Committee and the successful negotiation of a contract. A Statement of Appeal Rights has been provided with this letter; see below.

Thank you for your interest in doing business with the State of Maine.

Sincerely,

Signed by:
Lisa Leahy
E43B9746D9D144A...

Lisa Leahy
Director of Digital Services
lisa.leahy@maine.gov

STATEMENT OF APPEAL RIGHTS

Any person aggrieved by an award decision may request an appeal hearing. The request must be made to the Director of the Bureau of General Services, in writing, within 15 days of notification of the contract award as provided in 5 M.R.S. § 1825-E (2) and the Rules of the Department of Administrative and Financial Services, Bureau of General Services, Division of Purchases, Chapter 120, § (2) (2).

STATE OF MAINE
DEPARTMENT OF Administrative
and Financial Services

Janet T. Mills
Governor

Kirsten Figueroa
Commissioner

AWARD NOTIFICATION LETTER

August 7, 2024

Servos LLC
Sadie Loving
1704 Altamont Avenue
Richmond, VA, 23230
sloving@servos.io

SUBJECT: Notice of Conditional Contract Award under RFP # 202401005, Improve Delivery of Digital Services to Constituents

Dear Sadie:

This letter is in regard to the subject Request for Proposals (RFP), issued by the State of Maine Department of Administrative and Financial Services to Improve Delivery of Digital Services to Constituents. The Department has evaluated the proposals received using the evaluation criteria identified in the RFP, and the Department is hereby announcing its conditional contract award to the following bidder:

- Maine Information Network, LLC dba Tyler Maine

The bidder listed above received the evaluation team's highest ranking. The Department will be contacting the aforementioned bidder soon to negotiate a contract. As provided in the RFP, the Notice of Conditional Contract Award is subject to execution of a written contract and, as a result, this Notice does NOT constitute the formation of a contract between the Department and the apparent successful vendor. The vendor shall not acquire any legal or equitable rights relative to the contract services until a contract containing terms and conditions acceptable to the Department is executed. The Department further reserves the right to cancel this Notice of Conditional Contract Award at any time prior to the execution of a written contract.

As stated in the RFP, following announcement of this award decision, all submissions in response to the RFP are considered public records available for public inspection pursuant to

the State of Maine Freedom of Access Act (FOAA). 1 M.R.S. §§ 401 et seq.; 5 M.R.S. § 1825-B (6).

This award decision is conditioned upon final approval by the State Procurement Review Committee and the successful negotiation of a contract. A Statement of Appeal Rights has been provided with this letter; see below.

Thank you for your interest in doing business with the State of Maine.

Sincerely,

Signed by:
Lisa Leahy
E43B9746D9D144A...

Lisa Leahy
Director of Digital Services
lisa.leahy@maine.gov

STATEMENT OF APPEAL RIGHTS

Any person aggrieved by an award decision may request an appeal hearing. The request must be made to the Director of the Bureau of General Services, in writing, within 15 days of notification of the contract award as provided in 5 M.R.S. § 1825-E (2) and the Rules of the Department of Administrative and Financial Services, Bureau of General Services, Division of Purchases, Chapter 120, § (2) (2).

STATE OF MAINE
DEPARTMENT OF Administrative
and Financial Services

Janet T. Mills
Governor

Kirsten Figueroa
Commissioner

AWARD NOTIFICATION LETTER

August 7, 2024

Maine Information Network, LLC dba Tyler Maine
Samuel Foster
45 Commerce Drive, Suite 10
Augusta, ME, 04330
Samuel.foster@tylertech.com

SUBJECT: Notice of Conditional Contract Award under RFP # 202401005, Improve Delivery of Digital Services to Constituents

Dear Samuel:

This letter is in regard to the subject Request for Proposals (RFP), issued by the State of Maine Department of Administrative and Financial Services to Improve Delivery of Digital Services to Constituents. The Department has evaluated the proposals received using the evaluation criteria identified in the RFP, and the Department is hereby announcing its conditional contract award to the following bidder:

- Maine Information Network, LLC dba Tyler Maine

The bidder listed above received the evaluation team's highest ranking. The Department will be contacting the aforementioned bidder soon to negotiate a contract. As provided in the RFP, the Notice of Conditional Contract Award is subject to execution of a written contract and, as a result, this Notice does NOT constitute the formation of a contract between the Department and the apparent successful vendor. The vendor shall not acquire any legal or equitable rights relative to the contract services until a contract containing terms and conditions acceptable to the Department is executed. The Department further reserves the right to cancel this Notice of Conditional Contract Award at any time prior to the execution of a written contract.

As stated in the RFP, following announcement of this award decision, all submissions in response to the RFP are considered public records available for public inspection pursuant to

the State of Maine Freedom of Access Act (FOAA). 1 M.R.S. §§ 401 et seq.; 5 M.R.S. § 1825-B (6).

This award decision is conditioned upon final approval by the State Procurement Review Committee and the successful negotiation of a contract. A Statement of Appeal Rights has been provided with this letter; see below.

Thank you for your interest in doing business with the State of Maine.

Sincerely,

Signed by:
Lisa Leahy
E43B9746D9D144A...

Lisa Leahy
Director of Digital Services
lisa.leahy@maine.gov

STATEMENT OF APPEAL RIGHTS

Any person aggrieved by an award decision may request an appeal hearing. The request must be made to the Director of the Bureau of General Services, in writing, within 15 days of notification of the contract award as provided in 5 M.R.S. § 1825-E (2) and the Rules of the Department of Administrative and Financial Services, Bureau of General Services, Division of Purchases, Chapter 120, § (2) (2).

Team Consensus
Evaluation Notes

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Active Cyber
DATE: 06/12/2024

SUMMARY PAGE

Department Name: Department of Administrative and Financial Services
Name of RFP Coordinator: Lisa Leahy
Names of Evaluators: Dave Pascarella, Victor Chakravarty, Craig Locke, Lisa Leahy

---

Pass/Fail Criteria	Pass	Fail
Section I. Preliminary Information (Eligibility)	**X**	
Scoring Sections (Edit sections below to match evaluation criteria within RFP)	Points Available	Points Awarded
Section II. Organization Qualifications and Experience	**25**	**3**
Section III. Proposed Services	**50**	**17**
Section IV. Cost Proposal	**25**	**15.59**
Total Points	**100**	**35.59**

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Active Cyber
DATE: 06/12/2024

OVERVIEW OF SECTION I
Preliminary Information

Section I. Preliminary Information

Evaluation Team Comments:

PASS

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Active Cyber
DATE: 06/12/2024

EVALUATION OF SECTION II
Organization Qualifications and Experience

	Points Available	Points Awarded
Section II. Organization Qualifications and Experience	**25**	**3**

---

1. **Overview of the Organization (App. D)**

   Statement of qualifications
   - Does not meet requirements
     - No telephone or email info
     - Vague description of all 3 examples

2. **Subcontractors (App. E)**
   - No response

3. **Organizational Chart (No Appendix)**
   - No response

4. **Litigation (No App.)**
   - No response

5. **Financial Viability (No App.)**
   - No response

6. **Licensure/Certification (No App.)**
   - No response

7. **Certificate of Insurance (No App.)**
   - No response

Consensus:
- Does not meet requirements
  - Only answered 1 of 7

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Active Cyber
DATE: 06/12/2024

EVALUATION OF SECTION III
Proposed Services

	Points Available	Points Awarded
Section III. Proposed Services (File #3 – App. F, G, H)	**50**	**17**

1. **Technical Assessment (App. F)**
   ☒Done
   - **Did not meet Technical Requirements**

2. **Services to be Provided (App. G)**

	1. System security components Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.
	2. Identity Proofing Consensus: • Meets all requirements • The bidder marked this as an add on o Verified in cost form this is accommodated for • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements. o Proofing done by ID.ME
	3. Multi-factor authentication Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Active Cyber
DATE: 06/12/2024

4. **Risk-based factors**

Consensus:

- Meets all requirements
- Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.

5. **Identity lifecycle management components**

Consensus:

- Meets all requirements
- Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.

6. **Security event logging**

Consensus:

- Does not meet requirements
    - Only mentioned 1 of 2 products, Okta not ID.ME

7. **Security Certifications**

Consensus:

- Does not meet requirements
    - Only mentioned 1 of 2 products, Okta not ID.ME

8. **SIEM (Splunk) integration**

Consensus:

- Does not meet requirements
    - Only mentioned 1 of 2 products, Okta not ID.ME

9. **Core constituent data.**

Consensus:

- Does not meet requirements
    - Only mentioned 1 of 2 products, Okta not ID.ME
    - Unclear if data is external source, how does this store a citizen’s profile?

11. **Data Management.**

Consensus:

- Does not meet requirements
    - Only mentioned 1 of 2 products, Okta not ID.ME
    - Mention of partial but unsure of what this means

12. **SOM Employee.**

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Active Cyber
DATE: 06/12/2024

Consensus:

- Meets all requirements
- Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.

13. APIs.

Consensus:

- Meets all requirements
- Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.

14. User identification matching.

Consensus:

- Meets all requirements
- Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.

15. Single sign-on.

Consensus:

- Meets all requirements
- Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.

16. Import user profile data from agency systems

Consensus:

- Meets all requirements

17. History logging.

Consensus:

- Does not meet requirements
  - Only mentioned 1 of 2 products, Okta not ID.ME

18. Reporting.

Consensus:

- Does not meet requirements
  - Only mentioned 1 of 2 products, Okta not ID.ME

19. Security Controls. The system must comply to the following security controls:

Consensus:

- Does not meet requirements

	○ Only mentioned 1 of 2 products, Okta not ID.ME
	20. General System Requirements. Consensus: • Does not meet requirements ○ Only mentioned 1 of 2 products, Okta not ID.ME
	21. Training and Support. Consensus: • Does not meet requirements ○ Only mentioned 1 of 2 products, Okta not ID.ME
	22. Support Requirements Consensus: • Does not meet requirements ○ Only mentioned 1 of 2 products, Okta not ID.ME
	23. Hosting Consensus: • Does not meet requirements ○ Only mentioned 1 of 2 products, Okta not ID.ME
	24. Disaster Recovery Consensus: • Does not meet requirements ○ Only mentioned 1 of 2 products, Okta not ID.ME ○ In 2 of the 6 questions response was partial with no explanation.

3. **Response to Proposed Services (App. H - RFP pgs. 8-14)**

1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
Consensus:

- **Does not meet requirements**
  - **1 paragraph description is not a full description**
  - **Didn’t callout specific requirements**

1b) Detailed description of the technologies, software and / or hardware for each of the components.
Consensus:

- **Does not meet requirements**
  - **sparse description is not a full description**

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Active Cyber
DATE: 06/12/2024

1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.

Consensus:

- **Does not meet requirements**
  - **3 bullets of description is not a full description**

1d) Description of the overall platform and architecture of the proposed solution(s).

Consensus:

- **Does not meet requirements**
  - **1 paragraph description is not a full description**

1e) Description of any third-party software or partnerships required for the proposed Solution(s).

Consensus:

- **Does not meet requirements**
  - **sparse description is not a full description**

2a) A detailed timeline and description of milestones, deliverables, tasks

Consensus:

- **Does not meet requirements**
  - **Timeline and description inadequate**

2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period

Consensus:

- **Does not meet requirements**
  - **Resumes not included**
    - **No named resources**
  - **Roles and responsibilities meet requirements**
  - **Description of plan as 1 bullet item under each is not adequate**

2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.

Consensus:

- **Does not meet requirements**
  - **Deliverables generically listed,**
  - **No detailed work plan**
  - **No reference to personalized dashboard recommendations.**
  - **Implementation (MVP) is 6 month go live. Not detailed.**
  - **Tasks and milestones not clearly defined.**

2d) Average time to market for each component.

Consensus:

- **Does not meet requirements**
  - **Only 1 product mentioned (Okta not ID.ME)**
    - **Irrelevant response**

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

Consensus:

- **Meets all requirements for a. b. c. e. g. i.**
- **Does not meet requirements for d. f. h.**
  - **didn't speak to SOM specific**
  - **d. irrelevant response, doesn't answer the question**
    - **mentioned "integration with anything we have existing today."**
  - **f. irrelevant response, doesn't answer question**
  - **h. irrelevant response, no mention of consent**

B.2. The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.

Consensus:

- **Does not meet requirements**
    - **Bidder referenced being inspired by i.login but lacks detail.**

a. Disclosure and Consent Management

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**
    - **Opt-in, opt-out**
    - **Ability to set preference**
    - **Version history**
    - **User support**

b. Recommendation Technology

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

c. Data Management

Consensus:

- **Meets all requirements i. ii. iii. iv.**
    - **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**
- **Does not meet requirements v. vi.**
    - **mentions Okta but not ID.ME**

d. Customer Service

Consensus:

- **Does not meet requirements**
  - **"Deploy a sophisticated chatbot"**
    - **No specifics on which product**
  - **"24/7 phone support":**
    - **By whom?**

C.1. General System

Consensus:

- **Does not meet requirements**
  - **Only 1 product mentioned (Okta not ID.ME)**
    - **ID.ME phone app pictures, but no response**

C.2. Compliance with MaineIT Policies & Standards

Consensus:

- **Does not meet requirements**
  - **Response does not cover the question. (Web Standards, Digital Accessibility specifically aren't mentioned)**

C.3. Support and Maintenance

a. Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State's official acceptance of the implemented solution.

Consensus:

- **Does not meet requirements**
  - **Introduces a dedicated support partner that isn't mentioned at any other point**
    - **No details on support partner**
  - **AI powered chatbot lacks details**

b. Terms and duration of the support and maintenance will be specified in the contract.
Consensus:
- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

c. All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
Consensus:
- **No Response**

d. Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
Consensus:
- **Does not meet requirements**
  - **No details on support partner**

e. All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
Consensus:
- **Does not meet requirements**
  - **Only 1 product mentioned (Okta not ID.ME)**

f. All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
Consensus:
- **Does not meet requirements**
  - **Only 1 product mentioned (Okta not ID.ME)**

g. User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
Consensus:
- **Does not meet requirements**
  - **Only 1 product mentioned (Okta not ID.ME)**

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Active Cyber
DATE: 06/12/2024

4. Security

Consensus:

- Does not meet requirements
  - Only 1 product mentioned (Okta not ID.ME)

5. Licensing

Consensus:

- Does not meet requirements
  - Nothing is described in the section

1. Training and OCM (Organizational Change Management)

Consensus:

- Does not meet requirements
  - Did not address Security training
  - Did not address IAM training

2. Disaster Recovery

Consensus:

- Does not meet requirements
  - Only 1 product mentioned (Okta not ID.ME)
  - Does not meet RTO requirements

3. Feature Enhancements

Consensus:

- Meets all requirements
- Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.

4. Project Management

Consensus:

- Did not meet requirements
  - Did not provide specifics and only repeated what was asked

D. Value Added Options (Other)

Consensus:

- No response

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Active Cyber
DATE: 06/12/2024

EVALUATION OF SECTION IV
Cost Proposal

Lowest Submitted Cost Proposal	÷	Cost Proposal Being Scored	x	Score Weight	=	Score
20,017,462.34	**÷**	**32,091,320.00**	**x**	**25 points**	**=**	**15.59**

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Carahsoft
DATE: 06/12/2024

SUMMARY PAGE

Department Name: Department of Administrative and Financial Services
Name of RFP Coordinator: Lisa Leahy
Names of Evaluators: Dave Pascarella, Victor Chakravarty, Craig Locke, Lisa Leahy

---

Pass/Fail Criteria	Pass	Fail
Section I. Preliminary Information (Eligibility)	**X**	
Scoring Sections (Edit sections below to match evaluation criteria within RFP)	Points Available	Points Awarded
Section II. Organization Qualifications and Experience	**25**	**5**
Section III. Proposed Services	**50**	**10**
Section IV. Cost Proposal	**25**	**22.22**
Total Points	**100**	**37.22**

REV 4/4/2023

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Carahsoft
DATE: 06/12/2024

OVERVIEW OF SECTION I
Preliminary Information

Section I. Preliminary Information

Evaluation Team Comments:

PASS

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Carahsoft
DATE: 06/12/2024

EVALUATION OF SECTION II
Organization Qualifications and Experience

	Points Available	Points Awarded
Section II. Organization Qualifications and Experience	**25**	**5**

---

1. **Overview of the Organization (App. D)**

   Statement of qualifications
   - Does not meet requirements, closest relevant example is Services Australia
     - No contact information provided
       - Only 1 name
     - Lacking detail
       - All examples were blank in our checkboxes
     - Removed our template
     - Specificity of product and subcontractor references and contributions unclear

2. **Subcontractors (App. E)**
   - Does not meet requirements
     - Appendix c states Adobe as the bidder
       - Confusion as to who the bidder is, Carahsoft or Adobe?
     - Confusing response
     - Specificity of product and subcontractor references and contributions unclear

3. **Organizational Chart (No Appendix)**
   - No Org Chart provided
     - Vague list of position titles

4. **Litigation (No App.)**
   - Meets all requirements (for Carahsoft but not Adobe)

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Carahsoft
DATE: 06/12/2024

5. **Financial Viability (No App.)**
    - No D&B
        - Provided Carahsoft's latest annual revenue is 16.4 billion dollars
        - Provided info on a line of credit (25 million dollars)

6. **Licensure/Certification (No App.)**
    - Meets all requirements (for Adobe but not Carahsoft)

7. **Certificate of Insurance (No App.)**
    - Meets all requirements (for Carahsoft but not Adobe)
        - 5-million-dollar cyber liability

Consensus:

- While litigation, financial viability, and licensure meets requirements based on Carahsoft, there is confusion on subcontractors.

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Carahsoft
DATE: 06/12/2024

EVALUATION OF SECTION III
Proposed Services

	Points Available	Points Awarded
Section III. Proposed Services (File #3 – App. F, G, H)	**50**	**10**

1. **Technical Assessment (App. F)**
   ☒Done
   - **Did not meet Technical Requirements**

2. **Services to be Provided (App. G)**

	1. System security components Consensus: • Does not meet requirements o Response states they can but provides no explanation or supporting evidence.
	2. Identity Proofing Consensus: • Does not meet requirements o Does not define various levels of ID proofing directly
	3. Multi-factor authentication Consensus: • Does not meet requirements o Not specific o Didn't state the technology
	4. Risk-based factors Consensus: • Does not meet requirements o AI bot detection included o No specifics on device and location

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Carahsoft
DATE: 06/12/2024

	5. Identity lifecycle management components Consensus: • Meets all requirements

	6. Security event logging Consensus: • Does not meet requirements • No explanation • No evidence
	7. Security Certifications Consensus: • 1) Partial meets requirements with no explanation • 2) Cannot meet requirements with no explanation • No acknowledgement of IRS 45-day letter
	8. SIEM (Splunk) integration Consensus: • Does not meet requirements • No explanation • No evidence
	9. Core constituent data. Consensus: • Does not meet requirements • No explanation • No evidence
	11. Data Management. Consensus: • Does not meet requirements • No explanation • No evidence
	12. SOM Employee. Consensus: • Does not meet requirements • No explanation • No evidence

	13. APIs.

	Consensus: • Does not meet requirements • No explanation • No evidence
	14. User identification matching. Consensus: • Does not meet requirements • No explanation • No evidence
	15. Single sign-on. Consensus: • Does not meet requirements • No explanation • No evidence
	16. Import user profile data from agency systems Consensus: • Does not meet requirements • No explanation • No evidence
	17. History logging. Consensus: • Does not meet requirements • No explanation • No evidence
	18. Reporting. Consensus: • Does not meet requirements • No explanation • No evidence
	19. Security Controls. Consensus: • Does not meet requirements • No explanation • No evidence
	20. General System Requirements. Consensus: • Does not meet requirements • No explanation

	• No evidence
	21. Training and Support. Consensus: • Does not meet requirements • No explanation • No evidence
	22. Support Requirements Consensus: • Does not meet requirement • No explanation • No evidence
	23. Hosting Consensus: • Does not meet requirements • No explanation • No evidence
	24. Disaster Recovery Consensus: • Does not meet requirements • 5) bidder states partially meet requirements with no evidence • No explanation • No evidence

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.

Consensus:

- **Does not meet requirements**
    - **Incomplete response**
    - **Lacks detail of multiple parties' participation**

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Carahsoft
DATE: 06/12/2024

1b) Detailed description of the technologies, software and / or hardware for each of the components.

Consensus:

- **Does not meet requirements**
    - **Incomplete response**
    - **Lacks detail of multiple parties' participation**

1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.

Consensus:

- **Does not meet requirements**
    - **Incomplete response**
    - **Lacks detail of multiple parties' participation**

1d) Description of the overall platform and architecture of the proposed solution(s).

Consensus:

- **Does not meet requirements**
    - **Incomplete response**
    - **Lacks detail of multiple parties' participation**

1e) Description of any third-party software or partnerships required for the proposed Solution(s).

Consensus:

- **Does not meet requirements**
    - **Incomplete response**
    - **Lacks detail of multiple parties' participation**

2a) A detailed timeline and description of milestones, deliverables, tasks

Consensus:

- **No Response**

2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period

Consensus:

- **No Response**

2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.

Consensus:

- **No Response**

2d) Average time to market for each component.

Consensus:

- **No Response**

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

Consensus:

- **Meets all requirements for a. b. c. d. f. i.**
- **Does not meet requirements for e. g.**
- **No response for h.**

B.2. The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

a. Disclosure and Consent Management

Consensus:

- **Meets all requirements i. – iv.**
- **No response v. vi.**

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Carahsoft
DATE: 06/12/2024

b. Recommendation Technology

Consensus:

- **Partially meets requirements for i.**
- **No response ii.**
- **No response iii.**

c. Data Management

Consensus:

- **Does not meet requirements**
  - **Confusing responses**

d. Customer Service

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

C.1. General System

Consensus:

- **Meets all requirements**

C.2. Compliance with MaineIT Policies & Standards

Consensus:

- **Does not meet requirements**
  - **No evidence**
  - **No explanation**

C.3. Support and Maintenance

a. Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State’s official acceptance of the implemented solution.

Consensus:

- **Does not meet requirements**
  - **Adobe & Ping was covered but not OneTrust**

b. Terms and duration of the support and maintenance will be specified in the contract.
Consensus:
- **Does not meet requirements**
    - **Adobe & Ping was covered but not OneTrust**

c. All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
Consensus:
- **Does not meet requirements**
    - **Adobe & Ping was covered but not OneTrust**

d. Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
Consensus:
- **Does not meet requirements**
    - **Adobe & Ping was covered but not OneTrust**
    - **Didn’t mention toll free**

e. All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
Consensus:
- **No response**

f. All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
Consensus:
- **Does not meet requirements**
    - **Adobe was covered but not Ping & OneTrust**
        - **Didn’t say bidder would implement**

g. User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
Consensus:
- **Does not meet requirements**
    - **Adobe & Ping was covered but not OneTrust**

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Carahsoft
DATE: 06/12/2024

4. Security

Consensus:

- Does not meet requirements
  - Partially covers Adobe & Ping but not OneTrust
  - Appendix G does not cover everything that is being requested

5. Licensing

Consensus:

- Does not meet requirements
  - Nothing is described in the section

1. Training and OCM (Organizational Change Management)

Consensus:

- Meets all requirements for a. b. c.
- No response for d.

2. Disaster Recovery

Consensus:

- Does not meet requirements
  - Only covers Ping, Not Adobe & OneTrust
    - Ping response doesn't meet requirements

3. Feature Enhancements

Consensus:

- Meets all requirements

4. Project Management

Consensus:

- Does not meet requirements
  - Unclear, confusing. (mention of Salesforce?)
  - Boiler plate responses with nothing specific about this project.
  - Milestones and deliverables do not meet requirements
  - No mention of governance or document management

D. Value Added Options (Other)

Consensus:

- 1 option provided

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Carahsoft
DATE: 06/12/2024

EVALUATION OF SECTION IV
Cost Proposal

Lowest Submitted Cost Proposal	÷	Cost Proposal Being Scored	x	Score Weight	=	Score
20,017,462.34	÷	**22,521,533.82**	**x**	**25 points**	**=**	**22.22**

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Deloitte
DATE: 06/12/2024

SUMMARY PAGE

Department Name: Department of Administrative and Financial Services
Name of RFP Coordinator: Lisa Leahy
Names of Evaluators: Dave Pascarella, Victor Chakravarty, Craig Locke, Lisa Leahy

---

Pass/Fail Criteria	Pass	Fail
Section I. Preliminary Information (Eligibility)	**X**	
Scoring Sections (Edit sections below to match evaluation criteria within RFP)	Points Available	Points Awarded
Section II. Organization Qualifications and Experience	**25**	**1**
Section III. Proposed Services	**50**	**40**
Section IV. Cost Proposal	**25**	**14.32**
Total Points	**100**	**55.32**

REV 4/4/2023

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Deloitte
DATE: 06/12/2024

OVERVIEW OF SECTION I
Preliminary Information

Section I. Preliminary Information

Evaluation Team Comments:

PASS

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Deloitte
DATE: 06/12/2024

EVALUATION OF SECTION II
Organization Qualifications and Experience

	Points Available	Points Awarded
Section II. Organization Qualifications and Experience	**25**	**1**

- **Please note vendor submission did not include file #2**

1. **Overview of the Organization (App. D)**
   Statement of qualifications
   - Mention 5 states in appendix H (Texas, Kentucky, Michigan, Connecticut, Colorado)
   - Lot of history with the State

2. **Subcontractors (App. E)**
   - No response

3. **Organizational Chart (No Appendix)**
   - Meets all requirements
     - In appendix H

4. **Litigation (No App.)**
   - No response

5. **Financial Viability (No App.)**
   - No response

6. **Licensure/Certification (No App.)**
   - No response

7. **Certificate of Insurance (No App.)**
   - No response

Consensus:
- Does not meet requirements
- Cannot evaluate on documentation not provided

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Deloitte
DATE: 06/12/2024

EVALUATION OF SECTION III
Proposed Services

	Points Available	Points Awarded
Section III. Proposed Services (File #3 – App. F, G, H)	**50**	**40**

1. **Technical Assessment (App. F)**
   ☒Done
   - **Met Technical Requirements**

2. **Services to be Provided (App. G)**

	1. System security components Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.
	2. Identity Proofing Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.
	3. Multi-factor authentication Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.
	4. Risk-based factors Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Deloitte
DATE: 06/12/2024

	5. Identity lifecycle management components Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements. • No mention of offboarding

	6. Security event logging Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.
	7. Security Certifications Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements. • Mentions all 3 products • Did not explicitly say yes, but understand the 45-day IRS letter
	8. SIEM (Splunk) integration Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.
	9. Core constituent data. Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.
	11. Data Management. Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.
	12. SOM Employee. Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.

	13. APIs. Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements. ○ Specifically mentions will do one application
	14. User identification matching. Consensus: • Meets all requirements
	15. Single sign-on. Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.
	16. Import user profile data from agency systems. Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.
	17. History logging. Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.
	18. Reporting. Consensus: • Meets all requirements ○ Didn’t explicitly state it was available to dashboard
	19. Security Controls. Consensus: • Does not meet requirements ○ Inconsistent answers ○ Non-uniform coverage of products

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Deloitte
DATE: 06/12/2024

	20. General System Requirements. Consensus: • Meets all requirements o Assumption that only the admin mobile app is in native mode
	21. Training and Support. Consensus: • Does not meet requirements o Mentions Okta but not Salesforce or Socure o 1 Okta admin trained per contract term
	22. Support Requirements Consensus: • Meets all requirements o Confusing verbiage in appendix G about 2 week “hyper care” support and maintenance. Explanation found in appendix H o Product enhancements not included in 5)
	23. Hosting Consensus: • Does not meet requirements o Responds only to a) not b) o The response to a) is weak
	24. Disaster Recovery Consensus: • Meets all requirements o “Will facilitate conversation” is concerning language

3. **Response to Proposed Services (App. H - RFP pgs. 8-14)**

1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Deloitte
DATE: 06/12/2024

1b) Detailed description of the technologies, software and / or hardware for each of the components.

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

1d) Description of the overall platform and architecture of the proposed solution(s).

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

1e) Description of any third-party software or partnerships required for the proposed Solution(s).

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**
    - **Confusion about recommendation engine cost (Google Analytics)**

2a) A detailed timeline and description of milestones, deliverables, tasks

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

2d) Average time to market for each component.

Consensus:

- **Meets all requirements**
    - **Milestone chart covers this**

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

B.2. The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

a. Disclosure and Consent Management

Consensus:

- **Meets all requirements**

b. Recommendation Technology

Consensus:

- **Meets all requirements for i.**
- **Does not meet requirements for ii. & iii.**
    - **Confusion about recommendation engine**

c. Data Management

Consensus:

- **Meets all requirements for i. ii. iii.**
    - **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**
- **Does not meet requirements for iv. v. vi.**
    - **Covers Okta and Salesforce but not Socure**

d. Customer Service

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**
    - **Currently supports multiple States**

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Deloitte
DATE: 06/12/2024

C.1. General System

Consensus:

- **Meets all requirements**
    - **Assumption that only the admin mobile app is in native mode**

C.2. Compliance with MaineIT Policies & Standards

Consensus:

- **Meets all requirements**

C.3. Support and Maintenance

a. Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State's official acceptance of the implemented solution.
Consensus:
- **Meets all requirements**

b. Terms and duration of the support and maintenance will be specified in the contract.
Consensus:
- **Meets all requirements**

c. All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
Consensus:
- **Meets all requirements**

d. Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
Consensus:
- **Meets all requirements**

e. All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
Consensus:
- **Meets all requirements**

f. All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
Consensus:
- **Meets all requirements**

g. User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
Consensus:
- **Meets all requirements**

4. Security

Consensus:
- Meets all requirements
- Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.

5. Licensing

Consensus:
- Meets all requirements
- Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.

1. Training and OCM (Organizational Change Management)

Consensus:
- Meets all requirements
- Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.

2. Disaster Recovery

Consensus:
- Meets all requirements
- Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.
    - Inconsistency with answers in appendix G

3. Feature Enhancements

Consensus:
- Responded yes, meets requirements.

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Deloitte
DATE: 06/12/2024

4. Project Management

Consensus:

- Meets all requirements
- Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.

D. Value Added Options (Other)

Consensus:

- 3 Options provided

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Deloitte
DATE: 06/12/2024

EVALUATION OF SECTION IV
Cost Proposal

Lowest Submitted Cost Proposal	÷	Cost Proposal Being Scored	x	Score Weight	=	Score
20,017,462.34	**÷**	**34,935,517.34**	**x**	**25 points**	**=**	**14.32**

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Microsoft
DATE: 06/13/2024

SUMMARY PAGE

Department Name: Department of Administrative and Financial Services
Name of RFP Coordinator: Lisa Leahy
Names of Evaluators: Dave Pascarella, Victor Chakravarty, Craig Locke, Lisa Leahy

---

Pass/Fail Criteria	Pass	Fail
Section I. Preliminary Information (Eligibility)	**X**	
Scoring Sections (Edit sections below to match evaluation criteria within RFP)	Points Available	Points Awarded
Section II. Organization Qualifications and Experience	**25**	**11**
Section III. Proposed Services	**50**	**27**
Section IV. Cost Proposal	**25**	**25.00**
Total Points	**100**	**63.00**

REV 4/4/2023

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Microsoft
DATE: 06/13/2024

OVERVIEW OF SECTION I
Preliminary Information

Section I. Preliminary Information

Evaluation Team Comments:

PASS

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Microsoft
DATE: 06/13/2024

EVALUATION OF SECTION II
Organization Qualifications and Experience

	Points Available	Points Awarded
Section II. Organization Qualifications and Experience	**25**	**11**

---

1. **Overview of the Organization (App. D)**

   Statement of qualifications
   - Does not meet requirements
     - Didn't provide name + phone for contacts on listed projects
   - Long contract history with State

2. **Subcontractors (App. E)**
   - Meets all requirements
   - 2 subcontractors, provided all the details requested

3. **Organizational Chart (No Appendix)**
   - Meets all requirements

4. **Litigation (No App.)**
   - Does not meet requirements
     - Non-specific response

5. **Financial Viability (No App.)**
   - Does not meet requirements
     - No D&B

6. **Licensure/Certification (No App.)**
   - Meets all requirements
     - Strong global compliance portfolio

7. **Certificate of Insurance (No App.)**
   - No response

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Microsoft
DATE: 06/13/2024

EVALUATION OF SECTION III
Proposed Services

	Points Available	Points Awarded
Section III. Proposed Services (File #3 – App. F, G, H)	**50**	**27**

1. **Technical Assessment (App. F)**
   ☒Done
   - Met Technical Requirements

2. **Services to be Provided (App. G)**

	1. System security components Consensus: • Does not meet requirements • Lacking detail
	2. Identity Proofing Consensus: • Does not meet requirements • Lacking detail
	3. Multi-factor authentication Consensus: • Does not meet requirements • Lacking detail
	4. Risk-based factors Consensus: • Does not meet requirements • Lacking detail
	5. Identity lifecycle management components Consensus: • Does not meet requirements • Lacking detail

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Microsoft
DATE: 06/13/2024

	6. Security event logging Consensus: • Meets all requirements
	7. Security Certifications Consensus: • Does not meet requirements • Only talked about native stack NOT Socure • Acknowledged IRS 45-day letter
	8. SIEM (Splunk) integration Consensus: • Does not meet requirements • Only talked about native stack NOT Socure
	9. Core constituent data. Consensus: • Does not meet requirements o Lacking detail
	11. Data Management. Consensus: • Does not meet requirements o Lacking detail, just restated the question
	12. SOM Employee. Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.

	13. APIs. Consensus: • Meets all requirements
	14. User identification matching. Consensus: • Does not meet requirements • Lacking detail on function, just restated the question
	15. Single sign-on. Consensus: • Meets all requirements

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Microsoft
DATE: 06/13/2024

	16. Import user profile data from agency systems. Consensus: • Meets all requirements o No mention of offboarding
	17. History logging. Consensus: • Does not meet requirements o No details o Socure not mentioned
	18. Reporting. Consensus: • Meets all requirements
	19. Security Controls. Consensus: • Does not meet requirements o No mention of Socure
	20. General System Requirements. Consensus: • Meets all requirements
	21. Training and Support. Consensus: • Does not meet requirements o Non-committal
	22. Support Requirements Consensus: • Does not meet requirements o Non-committal
	23. Hosting Consensus: • Does not meet requirements o No mention of Socure in a)
	24. Disaster Recovery Consensus: • Meets all requirements

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Microsoft
DATE: 06/13/2024

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates a robust understanding and implementation of requirements.**

1b) Detailed description of the technologies, software and / or hardware for each of the components.

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates a robust understanding and implementation of requirements.**

1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates a robust understanding and implementation of requirements.**

1d) Description of the overall platform and architecture of the proposed solution(s).

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates a robust understanding and implementation of requirements.**

1e) Description of any third-party software or partnerships required for the proposed Solution(s).

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates a robust understanding and implementation of requirements.**

2a) A detailed timeline and description of milestones, deliverables, tasks

Consensus:

- **Meets all requirements**

2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period
Consensus:
- **Meets all requirements**

2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
Consensus:
- **Meets all requirements**

2d) Average time to market for each component.
Consensus:
- **Meets all requirements**

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. Capture Constituent Identity and profile data.
   Consensus:
   - **Meets all requirements**
   - **Provided a comprehensive response that demonstrates a robust understanding and implementation of requirements.**

b. Provide identity provisioning and deprovisioning.
   Consensus:
   - **Meets all requirements**
   - **Provided a comprehensive response that demonstrates a robust understanding and implementation of requirements.**

c. Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
Consensus:
- **Meets all requirements**
- **Provided a comprehensive response that demonstrates a robust understanding and implementation of requirements.**

d. Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies.
Consensus:
- **Meets all requirements**
- **Provided a comprehensive response that demonstrates a robust understanding and implementation of requirements.**

e. Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
Consensus:
- **No response**

f. Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.
Consensus:
- **No response**

g. Allow for multiple role selections for the following identities:
  i. Individual
  ii. Business Owner
  iii. Support multiple identities for State employees that work with the portal in a support role:
    (a) SOM Employee identity and credentials for supporting the application.
    (b) Constituent identity and credentials to use the state services offered through the portal.
  iv. Multi role individual (Individual and Business Owner)
  Consensus:
  - **No response**

h. Have the ability to provide levels of proofing which will be directly tied to the Constituent's level of consent given.

Consensus:

- **No response**

i. Support multi-factor authentication to protect against user impersonation and credential theft.

Consensus:

- **Meets all requirements**

B.2. The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates a robust understanding and implementation of requirements.**

a. Disclosure and Consent Management

Consensus:

- **Meets all requirements i. ii. iii. iv.**
- **Does not meet requirements v. vi.**

b. Recommendation Technology

Consensus:

- **Meets all requirements i.**
- **No responses ii. iii.**

c. Data Management

Consensus:

- **Meets all requirements i. ii. iii. v. vi.**
- **No response iv.**

d. Customer Service

Consensus:

- **Meets all requirements**

C.1. General System

Consensus:

- **Meets all requirements**

C.2. Compliance with MaineIT Policies & Standards

Consensus:

- **Does not meet requirements**
- **Covers native stack, missing Socure**

C.3. Support and Maintenance

a. Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State's official acceptance of the implemented solution.

Consensus:

- **Does not meet requirements**
- **Covers native stack, missing Socure**

b. Terms and duration of the support and maintenance will be specified in the contract.

Consensus:

- **Does not meet requirements**
- **Covers native stack, missing Socure**

c. All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.

Consensus:

- **Does not meet requirements**
- **Covers native stack, missing Socure**

d. Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
Consensus:
- **Does not meet requirements**
  - **Covers native stack, missing Socure**

e. All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
Consensus:
- **Does not meet requirements**
  - **Covers native stack, missing Socure**

f. All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
Consensus:
- **Does not meet requirements**
  - **Covers native stack, missing Socure**

g. User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
Consensus:
- **Does not meet requirements**
  - **Covers native stack, missing Socure**

4. Security

Consensus:
- Does not meet requirements
  - Covers native stack, missing Socure

5. Licensing

Consensus:
- Meets all requirements

1. Training and OCM (Organizational Change Management)

Consensus:
- No response c.
- Meets all requirements otherwise

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Microsoft
DATE: 06/13/2024

2. Disaster Recovery

Consensus:

- Does not meet requirements
  - Covers native stack, no mention of Socure

3. Feature Enhancements

Consensus:

- Meets all requirements

4. Project Management

Consensus:

- Does not meet requirements
  - Do not provide details about their methodologies, governance
  - Do list PM roles & responsibilities
  - No response e.

D. Value Added Options (Other)

Consensus:

- Provided 1 option

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Microsoft
DATE: 06/13/2024

EVALUATION OF SECTION IV
Cost Proposal

Lowest Submitted Cost Proposal	÷	Cost Proposal Being Scored	x	Score Weight	=	Score
20,017,462.34	**÷**	**20,017,462.34**	**x**	**25 points**	**=**	**25**

REV 4/4/2023

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: PruTech
DATE: 06/13/2024

SUMMARY PAGE

Department Name: Department of Administrative and Financial Services
Name of RFP Coordinator: Lisa Leahy
Names of Evaluators: Dave Pascarella, Victor Chakravarty, Craig Locke, Lisa Leahy

---

Pass/Fail Criteria	Pass	Fail
Section I. Preliminary Information (Eligibility)	**X**	
Scoring Sections (Edit sections below to match evaluation criteria within RFP)	Points Available	Points Awarded
Section II. Organization Qualifications and Experience	**25**	**23**
Section III. Proposed Services	**50**	**19**
Section IV. Cost Proposal	**25**	**9.78**
Total Points	**100**	**51.78**

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: PruTech
DATE: 06/13/2024

OVERVIEW OF SECTION I
Preliminary Information

Section I. Preliminary Information

Evaluation Team Comments:

PASS

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: PruTech
DATE: 06/13/2024

EVALUATION OF SECTION II
Organization Qualifications and Experience

	Points Available	Points Awarded
Section II. Organization Qualifications and Experience	**25**	**23**

---

1. **Overview of the Organization (App. D)**

   Statement of qualifications
   - Meets all requirements
   - All details provided, Name, phone number

2. **Subcontractors (App. E)**
   - Meets all requirements
   - 2 subcontractors all details provided

3. **Organizational Chart (No Appendix)**
   - Meets all requirements

4. **Litigation (No App.)**
   - Meets all requirements
   - Explicitly no litigation

5. **Financial Viability (No App.)**
   - Meets all requirements
     - D&B provided

6. **Licensure/Certification (No App.)**
   - Meets all requirements (CMMI Lev 3, ISO 9001:2015, SOC 2 Type 2)
   - SOC 2 is from September 1st 2022 - August 31st 2023

7. **Certificate of Insurance (No App.)**
   - Meets all requirements
     - $10 million cyber liability

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: PruTech
DATE: 06/13/2024

EVALUATION OF SECTION III
Proposed Services

	Points Available	Points Awarded
Section III. Proposed Services (File #3 – App. F, G, H)	**50**	**19**

1. **Technical Assessment (App. F)**

   ☒Done
   - While this met Technical Requirements there is concern on the ability to deliver on proposed solution.

2. **Services to be Provided (App. G)**

	1. System security components Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.
	2. Identity Proofing Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.
	3. Multi-factor authentication Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.
	4. Risk-based factors Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: PruTech
DATE: 06/13/2024

	5. Identity lifecycle management components Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.

	6. Security event logging Consensus: • Meets all requirements
	7. Security Certifications Consensus: • Does not meet requirements • No IRS 45-day acknowledgement • No details on HIPPA & SOC 2 Type II in 3) & 4)
	8. SIEM (Splunk) integration Consensus: • Meets all requirements
	9. Core constituent data. Consensus: • Meets all requirements
	11. Data Management. Consensus: • Does not meet all requirements • No details for Thales
	12. SOM Employee Consensus: • Meets all requirements

	13. APIs. Consensus: • Does not meet all requirements o No explicit mention of APIs being able to connect to at least one service

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: PruTech
DATE: 06/13/2024

	14. User identification matching. Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.
	15. Single sign-on. Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.
	16. Import user profile data from agency systems. Consensus: • Meets all requirements
	17. History logging. Consensus: • Does not meet requirements • No mention of products
	18. Reporting. Consensus: • Does not meet requirements • No mention of Thales • Not visible to portal
	19. Security Controls. Consensus: • Does not meet requirements • Only mentions Okta not Thales
	20. General System Requirements Consensus: • Does not meet requirements • No mention of the portal/dashboard supporting browsers
	21. Training and Support. Consensus: • Meets all requirements
	22. Support Requirements Consensus: • Meets all requirements

	23. Hosting Consensus: • Does not meet requirements • No mention of Thales • No mention of dashboard
	24. Disaster Recovery Consensus: • Does not meet requirements • No mention of Thales • No mention of dashboard

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
Consensus:
- **Meets all requirements**

1b) Detailed description of the technologies, software and / or hardware for each of the components.
Consensus:
- **Meets all requirements**

1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.
Consensus:
- **Meets all requirements**

1d) Description of the overall platform and architecture of the proposed solution(s).
Consensus:
- **Meets all requirements**

1e) Description of any third-party software or partnerships required for the proposed Solution(s).
Consensus:
- **Meets all requirements**

2a) A detailed timeline and description of milestones, deliverables, tasks

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**
    - **15 months, included breakdown of deliverables and milestones**

2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**
    - **Completed all resumes, roles and responsibilities**

2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.

Consensus:

- **Does not meet requirements**
    - **No detailed work plan**

2d) Average time to market for each component.

Consensus:

- **No response**

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. Capture Constituent Identity and profile data.
Consensus:
- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

b. Provide identity provisioning and deprovisioning.
Consensus:
- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

c. Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
i. Identity Creation
ii. Identity provisioning
iii. Attribute maps
iv. Authentication (e.g., password policies and synchronization)
Consensus:
- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

d. Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies.
Consensus:
- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

e. Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
Consensus:
- **Meets all requirements**

- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

f. Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.
Consensus:
- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

g. Allow for multiple role selections for the following identities:
  i. Individual
  ii. Business Owner
  iii. Support multiple identities for State employees that work with the portal in a support role:
    (a) SOM Employee identity and credentials for supporting the application.
    (b) Constituent identity and credentials to use the state services offered through the portal.
  iv. Multi role individual (Individual and Business Owner)

Consensus:
- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

h. Have the ability to provide levels of proofing which will be directly tied to the Constituent’s level of consent given.
Consensus:
- **Irrelevant response**
- **Thought Thales was the proofing product**

i. Support multi-factor authentication to protect against user impersonation and credential theft.
Consensus:
- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

B.2. The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.

Consensus:

- **Meets all requirements**

a. Disclosure and Consent Management

Consensus:

- **Does not meet requirements**
  - **The only statement was that it is offered by their proposed solution without any detail.**

b. Recommendation Technology

Consensus:

- **Meets all requirements**

c. Data Management

Consensus:

- **Meets all requirements i. ii. iii. iv.**
- **Does not meet requirements v. & vi.**
  - **Mentions Okta but not Thales**

d. Customer Service

Consensus:

- **Meets all requirements**

C.1. General System

Consensus:

- **Does not meet requirements**
  - **b. only mentions Okta not Thales**
  - **a. & d. No mention of the portal/dashboard**

C.2. Compliance with MaineIT Policies & Standards

Consensus:

- **Does not meet requirements**
    - **Mentions Okta, no Thales, no Portal**

C.3. Support and Maintenance

a. Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State's official acceptance of the implemented solution.

Consensus:

- **Meets all requirements**

b. Terms and duration of the support and maintenance will be specified in the contract.

Consensus:

- **Meets all requirements**

c. All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.

Consensus:

- **Meets all requirements**

d. Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)

Consensus:

- **Meets all requirements**

e. All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.

Consensus:

- **Meets all requirements**

f. All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.

Consensus:

- **Meets all requirements**

g. User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.

Consensus:

- **Meets all requirements**

4. **Security**

Consensus:

- Does not meet requirements
  - Mentions Okta, no Thales, no Portal

5. **Licensing**

Consensus:

- Does not meet requirements
  - Nothing is described in the section

1. **Training and OCM (Organizational Change Management)**

Consensus:

- Does not meet requirements for c.
- Otherwise meets all requirements

2. **Disaster Recovery**

Consensus:

- Does not meet requirements
  - Mentions Okta, not Thales, not Portal

3. **Feature Enhancements**

Consensus:

- Responded yes, meets requirements

4. **Project Management**

Consensus:

- Does not meet requirements for a. b. c. d.
  - Lacking detail, sometimes with no response

  - Meets requirements for e.

D. Value Added Options (Other)

Consensus:

- Offered 1 value added option

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: PruTech
DATE: 06/13/2024

EVALUATION OF SECTION IV
Cost Proposal

Lowest Submitted Cost Proposal	÷	Cost Proposal Being Scored	x	Score Weight	=	Score
20,017,462.34	÷	**51,176,746.78**	**x**	**25 points**	**=**	**9.78**

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Servos
DATE: 06/13/2024

SUMMARY PAGE

Department Name: Department of Administrative and Financial Services
Name of RFP Coordinator: Lisa Leahy
Names of Evaluators: Dave Pascarella, Victor Chakravarty, Craig Locke, Lisa Leahy

---

Pass/Fail Criteria	Pass	Fail
Section I. Preliminary Information (Eligibility)	**X**	
Scoring Sections (Edit sections below to match evaluation criteria within RFP)	Points Available	Points Awarded
Section II. Organization Qualifications and Experience	**25**	**2**
Section III. Proposed Services	**50**	**8**
Section IV. Cost Proposal	**25**	**15.52**
Total Points	**100**	**25.52**

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Servos
DATE: 06/13/2024

OVERVIEW OF SECTION I
Preliminary Information

Section I. Preliminary Information

Evaluation Team Comments:

PASS

REV 4/4/2023

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Servos
DATE: 06/13/2024

EVALUATION OF SECTION II
Organization Qualifications and Experience

	Points Available	Points Awarded
Section II. Organization Qualifications and Experience	**25**	**2**

---

1. **Overview of the Organization (App. D)**

   Statement of qualifications
   - Does not meet requirements
     - Did not include competencies covered by each example
     - Provides names, emails, and 4 examples but doesn't go into details

2. **Subcontractors (App. E)**
   - None

3. **Organizational Chart (No Appendix)**
   - No response

4. **Litigation (No App.)**
   - No response

5. **Financial Viability (No App.)**
   - No response

6. **Licensure/Certification (No App.)**
   - No response

7. **Certificate of Insurance (No App.)**
   - No response

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Servos
DATE: 06/13/2024

EVALUATION OF SECTION III
Proposed Services

	Points Available	Points Awarded
Section III. Proposed Services (File #3 – App. F, G, H)	**50**	**8**

1. **Technical Assessment (App. F)**
   ☒Done
   - **Did not meet Technical Requirements**

2. **Services to be Provided (App. G)**

	1. System security components Consensus: • Does not meet requirements o No explanation for add on o Confusion over proposed products used in solution (ID.me vs ServiceNow)
	2. Identity Proofing Consensus: • Does not meet requirements o No explanation for add on o Confusion over proposed products used in solution (ID.me vs ServiceNow)
	3. Multi-factor authentication Consensus: • Meets all requirements but no explanation or evidence provided
	4. Risk-based factors Consensus: • Bidder responded partially meets requirements but response provides no explanation as to why

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Servos
DATE: 06/13/2024

	5. Identity lifecycle management components Consensus: • Does not meet requirements • Conflicting information between which product (ServiceNow or ID.me) is doing the identity lifecycle management

	6.Security event logging Consensus: • Does not meet requirements • No supporting evidence
	7. Security Certifications Consensus: • Does not meet requirements • Only mentions ServiceNow no mention of ID.me • No IRS 45-day acknowledgement
	8. SIEM (Splunk) integration Consensus: • Does not meet requirements • No explanation
	9. Core constituent data. Consensus: • Does not meet requirements • No explanation
	11. Data Management. Consensus: • Does not meet requirements • No explanation
	12. SOM Employee. Consensus: • Does not meet requirements • No explanation

	13. APIs. Consensus: • Does not meet requirements • No explanation

	14. User identification matching. Consensus: • Does not meet requirements • No explanation
	15. Single sign-on. Consensus: • Does not meet requirements • No explanation
	16. Import user profile data from agency systems. Consensus: • Does not meet requirements • No explanation
	17. History logging. Consensus: • Does not meet requirements • No explanation
	18. Reporting. Consensus: • Does not meet requirements • No explanation
	19. Security Controls. Consensus: • Does not meet requirements • Only mentions ServiceNow not ID.me
	20. General System Requirements. Consensus: • Does not meet requirements • No explanation
	21. Training and Support. Consensus: • Does not meet requirements • No explanation
	22. Support Requirements Consensus: • Does not meet requirements • No explanation

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Servos
DATE: 06/13/2024

	23. Hosting Consensus: • Does not meet requirements • Irrelevant explanation
	24. Disaster Recovery Consensus: • Does not meet requirements • Only mentions ServiceNow not ID.me

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
Consensus:
- **Meets all requirements**

1b) Detailed description of the technologies, software and / or hardware for each of the components.
Consensus:
- **Meets all requirements**

1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.
Consensus:
- **Meets all requirements**

1d) Description of the overall platform and architecture of the proposed solution(s).
Consensus:
- **Meets all requirements**

1e) Description of any third-party software or partnerships required for the proposed Solution(s).
Consensus:
- **Does not meet requirements**
- **Response does not mention ServiceNow**

2a) A detailed timeline and description of milestones, deliverables, tasks
Consensus:

- **Meets all requirements**

2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff ©, and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period
Consensus:

- **Meets all requirements**
- **Resumes are only from ServiceNow, nothing from ID.me**

2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
Consensus:

- **Meets all requirements**

2d) Average time to market for each component.
Consensus:

- **Meets all requirements**

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. Capture Constituent Identity and profile data.
Consensus:

- **Does not meet requirements**
- **Conflicting/inconsistent response as to distribution of labor between products (ServiceNow vs. ID.me)**
- **Fails to respond to the proposed CIAM solution of ServiceNow**

b. Provide identity provisioning and deprovisioning.
Consensus:
- **Does not meet requirements**
- **Conflicting/inconsistent response as to distribution of labor between products (ServiceNow vs. ID.me)**
- **Fails to respond to the proposed CIAM solution of ServiceNow**

c. Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
Consensus:
- **Does not meet requirements**
- **Conflicting/inconsistent response as to distribution of labor between products (ServiceNow vs. ID.me)**
- **Fails to respond to the proposed CIAM solution of ServiceNow**

d. Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies.
Consensus:
- **Does not meet requirements**
- **Conflicting/inconsistent response as to distribution of labor between products (ServiceNow vs. ID.me)**
- **Fails to respond to the proposed CIAM solution of ServiceNow**

e. Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
Consensus:
- **Does not meet requirements**
- **Conflicting/inconsistent response as to distribution of labor between products (ServiceNow vs. ID.me)**
- **Fails to respond to the proposed CIAM solution of ServiceNow**

f. Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.
Consensus:
- **Does not meet requirements**
- **Conflicting/inconsistent response as to distribution of labor between products (ServiceNow vs. ID.me)**
- **Fails to respond to the proposed CIAM solution of ServiceNow**

g. Allow for multiple role selections for the following identities:
    i. Individual
    ii. Business Owner
    iii. Support multiple identities for State employees that work with the portal in a support role:
        (a) SOM Employee identity and credentials for supporting the application.
        (b) Constituent identity and credentials to use the state services offered through the portal.
    iv. Multi role individual (Individual and Business Owner)

Consensus:

- **Does not meet requirements**
- **Conflicting/inconsistent response as to distribution of labor between products (ServiceNow vs. ID.me)**
- **Fails to respond to the proposed CIAM solution of ServiceNow**

h. Have the ability to provide levels of proofing which will be directly tied to the Constituent's level of consent given.

Consensus:

- **Does not meet requirements**
- **Conflicting/inconsistent response as to distribution of labor between products (ServiceNow vs. ID.me)**
- **Fails to respond to the proposed CIAM solution of ServiceNow**

i. Support multi-factor authentication to protect against user impersonation and credential theft.

Consensus:

- **Does not meet requirements**
- **Conflicting/inconsistent response as to distribution of labor between products (ServiceNow vs. ID.me)**
- **Fails to respond to the proposed CIAM solution of ServiceNow**

B.2. The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.

Consensus:
- **Does not meet requirements**
- **No mention that this is a ServiceNow portal**
- **Confusing details**

a. Disclosure and Consent Management

Consensus:
- **Does not meet requirements**
- **ID.me is now presented as the disclosure and consent management product**
- **No details on integration**
- **Conflicting/confusing information**

b. Recommendation Technology

Consensus:
- **Does not meet requirements**
- **Recommendation technology is ServiceNow**
- **Confusing/conflicting information**
- **Do not understand distribution of labor between products (ServiceNow vs ID.me)**

c. Data Management

Consensus:
- **Does not meet requirements**
- **Conflicting/confusing information**
- **All data management is through ServiceNow**
- **No mention of ID.me**

d. Customer Service

Consensus:
- **Does not meet requirements**
- **ServiceNow is the customer service provider**
- **No mention of ID.me support, no mention of portal/dashboard support**
- **No mention of toll-free number**

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Servos
DATE: 06/13/2024

C.1. General System

Consensus:

- **Does not meet requirements**
  - **Response for ServiceNow meets all requirements**
  - **No mention of ID.me, no mention of portal/dashboard support**

C.2. Compliance with MaineIT Policies & Standards

Consensus:

- **Does not meet requirements**
  - **Only mentions ServiceNow, not ID.me, not portal/dashboard**
  - **No mention of Accessibility Policy & Web Standards**

C.3. Support and Maintenance

a. Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State’s official acceptance of the implemented solution.

Consensus:

- **Does not meet requirements**
- **Confusing response, first paragraph uses language from bidder, second portion is from ServiceNow**

b. Terms and duration of the support and maintenance will be specified in the contract.

Consensus:

- **Does not meet requirements**
- **Confusing response, first paragraph uses language from bidder, second portion is from ServiceNow**

c. All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.

Consensus:

- **Does not meet requirements**
- **Confusing response, first paragraph uses language from bidder, second portion is from ServiceNow**

d. Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
Consensus:
- **Does not meet requirements**
- **Confusing response, first paragraph uses language from bidder, second portion is from ServiceNow**

e. All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
Consensus:
- **Does not meet requirements**
- **Confusing response, first paragraph uses language from bidder, second portion is from ServiceNow**

f. All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
Consensus:
- **Does not meet requirements**
- **Confusing response, first paragraph uses language from bidder, second portion is from ServiceNow**

g. User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
Consensus:
- **Does not meet requirements**
- **Confusing response, first paragraph uses language from bidder, second portion is from ServiceNow**

4. Security

Consensus:
- Does not meet requirements
  - Only mentions ServiceNow not ID.me
  - Does not cover all requirements from ServiceNow

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Servos
DATE: 06/13/2024

5. **Licensing**

   Consensus:
   - Does not meet requirements
     - Nothing is described in this section

1. **Training and OCM (Organizational Change Management)**

Consensus:
- Does not meet requirements
  - First 2 paragraphs do not provide answers to any requirements
  - Role confusion on who is doing the OCM (ServiceNow or Servos?)

2. **Disaster Recovery**

Consensus:
- Does not meet requirements
- Only mentions ServiceNow not ID.me
  - Never answered RPO or RTO

3. **Feature Enhancements**

   Consensus:
   - Response didn't address the requirements
   - Irrelevant response

4. **Project Management**

   Consensus:

   - Does not meet requirements
   - Did not address the requirements
   - Not enough detail

D. Value Added Options (Other)

Consensus:
- Provided one option

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Servos
DATE: 06/13/2024

EVALUATION OF SECTION IV
Cost Proposal

Lowest Submitted Cost Proposal	÷	Cost Proposal Being Scored	x	Score Weight	=	Score
20,017,462.34	**÷**	**32,250,725.00**	**x**	**25 points**	**=**	**15.52**

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Tyler Tech
DATE: 06/14/2024

SUMMARY PAGE

Department Name: Department of Administrative and Financial Services
Name of RFP Coordinator: Lisa Leahy
Names of Evaluators: Dave Pascarella, Victor Chakravarty, Craig Locke, Lisa Leahy

---

Pass/Fail Criteria	Pass	Fail
Section I. Preliminary Information (Eligibility)	**X**	
Scoring Sections (Edit sections below to match evaluation criteria within RFP)	Points Available	Points Awarded
Section II. Organization Qualifications and Experience	**25**	**22**
Section III. Proposed Services	**50**	**35**
Section IV. Cost Proposal	**25**	**18.34**
Total Points	**100**	**75.34**

REV 4/4/2023

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Tyler Tech
DATE: 06/14/2024

OVERVIEW OF SECTION I
Preliminary Information

Section I. Preliminary Information

Evaluation Team Comments:

PASS

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Tyler Tech
DATE: 06/14/2024

SUMMARY PAGE

Department Name: Department of Administrative and Financial Services
Name of RFP Coordinator: Lisa Leahy
Names of Evaluators: Dave Pascarella, Victor Chakravarty, Craig Locke, Lisa Leahy

---

Pass/Fail Criteria	Pass	Fail
Section I. Preliminary Information (Eligibility)	**X**	
Scoring Sections (Edit sections below to match evaluation criteria within RFP)	Points Available	Points Awarded
Section II. Organization Qualifications and Experience	**25**	**22**
Section III. Proposed Services	**50**	**35**
Section IV. Cost Proposal	**25**	**18.34**
Total Points	**100**	**75.34**

REV 4/4/2023

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Tyler Tech
DATE: 06/14/2024

OVERVIEW OF SECTION I
Preliminary Information

Section I. Preliminary Information

Evaluation Team Comments:

PASS

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Tyler Tech
DATE: 06/14/2024

EVALUATION OF SECTION II
Organization Qualifications and Experience

	Points Available	Points Awarded
Section II. Organization Qualifications and Experience	**25**	**22**

---

1. **Overview of the Organization (App. D)**

   Statement of qualifications
   - Meets all requirements
   - Provided 5 examples instead of 3
   - All contact details provided
   - Long history with the State
   - Presented local services already providing around the State
   - We asked for 6 competencies, bidder addressed all 6 competencies
   - The bidder provided a thorough description of their experience and qualifications relevant to the RFP requirements, demonstrating their capability to deliver on the project.

2. **Subcontractors (App. E)**
   - Meets all requirements
     - 1 Subcontractor; Socure
     - Contact details provided
     - Clear and crisp response that left no ambiguity with who is being brought in to assist with roles and responsibilities

3. **Organizational Chart (No Appendix)**
   - Provided meaningful/detailed Org Chart
   - Missing Socure, but clarified in demo

4. **Litigation (No App.)**
   - No active litigation cases in past 5 years

5. **Financial Viability (No App.)**
   - Meets all requirements
     - Complete D&B report provided with positive results and low risk

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Tyler Tech
DATE: 06/14/2024

6. Licensure/Certification (No App.)

- No response

7. Certificate of Insurance (No App.)

- Meets all requirements
    - $10 million cyber liability

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Tyler Tech
DATE: 06/14/2024

EVALUATION OF SECTION III
Proposed Services

	Points Available	Points Awarded
Section III. Proposed Services (File #3 – App. F, G, H)	**50**	**35**

1. **Technical Assessment (App. F)**

   ☒Done

   - Initially there was no clarification of Socure in App. F, this issue was later clarified in App G, H, and the demo.

2. **Services to be Provided (App. G)**

	1. System security components Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.
	2. Identity Proofing Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.
	3. Multi-factor authentication Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.
	4. Risk-based factors Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.
	5. Identity lifecycle management components Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Tyler Tech
DATE: 06/14/2024

	6. Security event logging Consensus: • Meets all requirements • Did not specifically mention Socure, but stated entirety of portal/platform
	7. Security Certifications Consensus: • Does not meet requirements • Irrelevant response, question is about the system not the bidder • No IRS 45-day acknowledgement
	8. SIEM (Splunk) integration Consensus: • Meets all requirements • Did not specifically mention Socure, but stated entirety of portal/platform
	9. Core constituent data Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.
	11. Data Management Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.
	12. SOM Employee Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.
	13. APIs Consensus: • Meets all requirements • LDAP not natively supported, requires addon
	14. User identification matching Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Tyler Tech
DATE: 06/14/2024

	15. Single sign-on Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.
	16. Import user profile data from agency systems Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.
	17. History logging Consensus: • Meets all requirements • Did not specifically mention Socure, but stated entirety of portal/platform
	18. Reporting Consensus: • Meets all requirements • Lacking detail on reporting from specific products
	19. Security Controls Consensus: • Does not meet all requirements • Question was about the system, not the bidder • No explicit mention of Drupal, Okta, Socure
	20. General System Requirements Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements. • Will build fully native mobile app, not just a redirect to a web browser app
	21. Training and Support Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.
	22. Support Requirements Consensus: • Meets all requirements • Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.

	23. Hosting Consensus: • Meets all requirements but lacks specificity of product's ability to meet Hosting requirements
	24. Disaster Recovery Consensus: • Meets all requirements but lacks specificity for each product's ability to meet Disaster Recovery timeframe

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**
    - **i. Highlighted experience with legacy services.**

1b) Detailed description of the technologies, software and / or hardware for each of the components.

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**
    - **i. Detailed description of resident engagement platform.**

1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

1d) Description of the overall platform and architecture of the proposed solution(s).

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Tyler Tech
DATE: 06/14/2024

1e) Description of any third-party software or partnerships required for the proposed Solution(s).

Consensus:

- **Meets all requirements**
  i. **Do not mention actual Socure subcontracting work**

2a) A detailed timeline and description of milestones, deliverables, tasks

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**
  i. **Milestones, deliverables, and tasks included**

2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period

Consensus:

- **Does not meet requirements**
  - **Missing Socure**
  - **Weak resumes**

2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.

Consensus:

- **Does not meet requirements**
  i. **Picture provided is lacking detail on the implementation and deliverables**

2d) Average time to market for each component.

Consensus:

- **No response**

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Tyler Tech
DATE: 06/14/2024

a. Capture Constituent Identity and profile data.

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

b. Provide identity provisioning and deprovisioning.

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

c. Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

d. Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies.

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

e. Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.

Consensus:

- **No response**

f. Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

g. Allow for multiple role selections for the following identities:
  i. Individual
  ii. Business Owner
  iii. Support multiple identities for State employees that work with the portal in a support role:
    (a) SOM Employee identity and credentials for supporting the application.
    (b) Constituent identity and credentials to use the state services offered through the portal.
  iv. Multi role individual (Individual and Business Owner)

Consensus:

- **Does not meet requirements**
  - **Lacking detail, covered i. didn’t cover ii. iii. iv.**

h. Have the ability to provide levels of proofing which will be directly tied to the Constituent’s level of consent given.

Consensus:

- **No response**

i. Support multi-factor authentication to protect against user impersonation and credential theft.

Consensus:

- **No response**

B.2. The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.

Consensus:

- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Tyler Tech
DATE: 06/14/2024

a. Disclosure and Consent Management
Consensus:
- **Meets all requirements for i. ii. iv. v. vi.**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**
- **Does not meet all requirements for iii.**
    - **Asked for interactive and set preference mode, only responded to interactive**

b. Recommendation Technology
Consensus:
- **Meets all requirements**
- **Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.**

c. Data Management
Consensus:
- **Meets all requirements for i. ii. iii. iv.**
- **Does not meet all requirements for v. vi.**
    - **Missing product details, generic statement that didn't speak to the actual question/requirements with specificity**

d. Customer Service
Consensus:
- **Meets all requirements**
    - **No explicit mention that bidder is doing customer service for all products**

C.1. General System
Consensus:
- **Meets all requirements**
    - **Confusion on products**

C.2. Compliance with MaineIT Policies & Standards
Consensus:
- **Does not meet all requirements**
    - **No mention of products, "open discussions with State" doesn't satisfy**

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Tyler Tech
DATE: 06/14/2024

C.3. Support and Maintenance

a. Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State's official acceptance of the implemented solution.
   Consensus:
   - **Meets all requirements**

b. Terms and duration of the support and maintenance will be specified in the contract.
   Consensus:
   - **Meets all requirements**

c. All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
   Consensus:
   - **Meets all requirements**

d. Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
   Consensus:
   - **Meets all requirements**

e. All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
   Consensus:
   - **Meets all requirements**

f. All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
   Consensus:
   - **Meets all requirements**

g. User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
   Consensus:
   - **Meets all requirements**

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Tyler Tech
DATE: 06/14/2024

4. Security

Consensus:

- Does not meet requirements
  - Missing Socure, which is a vital component of their security posture/proposal and is a required competency

5. Licensing

Consensus:

- Meets all requirements

1. Training and OCM (Organizational Change Management)

Consensus:

- Meets all requirements
  - Bidder proposed a training regiment that includes a step-by-step onboarding guide for agencies that takes into consideration the development of an agency readiness assessment form.

2. Disaster Recovery

Consensus:

- Meets all requirements
- Provided a comprehensive response that demonstrates robust understanding and implementation of requirements.

3. Feature Enhancements

Consensus:

Responded yes, meets requirements

4. Project Management

Consensus:

- Meets all requirements for a, b, c
- Does not meet requirements for d.
  - No mention of reporting
- Partially meets requirements for e.
  - internal and external communication plan
  - no quality management methodologies
  - overall governance is strong

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Tyler Tech
DATE: 06/14/2024

D. Value Added Options (Other)

Consensus:

- Provided 3 options

STATE OF MAINE
CONSENSUS EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services To Constituents
BIDDER: Tyler Tech
DATE: 06/14/2024

EVALUATION OF SECTION IV
Cost Proposal

Lowest Submitted Cost Proposal	÷	Cost Proposal Being Scored	x	Score Weight	=	Score
20,017,462.34	**÷**	**27,289,817.00**	**x**	**25 points**	**=**	**18.34**

REV 4/4/2023

Individual Evaluator Notes

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Active Cyber
DATE: 6/11/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

Section I – Preliminary Information (No points – Eligibility Requirements)

(File #1 App. A, B, C)
☒Done – Pass/Fail by Procurement & RFP Coordinator

Section II Organization Qualifications and Experience

(File #2 – App. D, E + other areas that have no Appendix number but are part of File #2)

1. **Overview of the Organization (App. D)**
   ☒Bidders must include three examples of projects which demonstrate their experience and expertise in performing these services as well as highlighting the Bidder's stated qualifications and skills.

   Statement of qualifications
   ☒Client name, contact person, Ph#, email.
   Contract history with the state may be considered in rating proposals even if not provided by the bidder.

   P, N, Q, or I & Notes:
   No contact information provided. States provided on down selection

2. **Subcontractors (App. E)**
   ☒If subcontractors are to be used, Bidders must provide the name, address, phone number, contact person, and a brief description of the subcontractors' organizational capacity and qualifications.
   Business name, contact person, address, ph#, email.
   P, N, Q, or I & Notes:P none

3. **Organizational Chart (No Appendix)**
   ☐Bidders must provide an organizational chart. The organizational chart must include the project being proposed. Each position must be identified by position title and corresponding to the personnel job descriptions.
   P, N, Q, or I & Notes:Q not found

4. **Litigation (No App.)**

☒Bidders must attach a list of all current litigation in which the Bidder is named and a list of all closed cases that have closed within the past five (5) years in which the Bidder paid the claimant either as part of a settlement or by decree. For each, list the entity bringing suit, the complaint, the accusation, amount, and outcome.
P, N, Q, or I & Notes: 3 years not 5 years

5. **Financial Viability (No App.)**
☐Bidders must provide a current copy of their Dun & Bradstreet Business Information Report Snapshot.
P, N, Q, or I - Notes: Q not found

6. **Licensure/Certification (No App.)**
☐Bidders *may* provide documentation of any applicable licensure/certification or specific credentials that are related to providing the proposed services of the RFP.
P, N, Q, or I & Notes: Q not found

7. **Certificate of Insurance (No App.)**
☐Bidders must provide a certificate of insurance on a standard ACORD form (or the equivalent) evidencing the Bidder's general liability, professional liability and any other relevant liability insurance policies that might be associated with the proposed services.
P, N, Q, or I & Notes: Q not found

Section III - Proposed Services

(File #3 – App. F, G, H)

1. **Technical Assessment (App. F)**
☒Done

2. **Services to be Provided (App. G)**

Note: on App. G Detailed Technical and Functional Requirements Excel spreadsheet, a tab is labeled User Stories. No response is required for Tab 3; these were provided to bidders for clarity and understanding of the expected journey a Constituent will experience.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Active Cyber
DATE: 6/11/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes:P	**1. System security components System security must include the following security components:**
	1) Account Take Over Protections
	a) Account Sign-in Protections
	a) Account Sign-in Protections
	a) Adaptive AI Technology
	b) Bot Protection: identify visitor behavior through analysis of technical and behavioral data.
☒ P, Q, N or I Notes: P	**2. Identity Proofing must have the ability to provide levels of proofing which will be directly tied to the constituent's level of access.**
	1) Define various levels of id proofing
	2) Document Image Capture
	3) Close coupling with authentication
☒ P, Q, N or I Notes: P	**3. Multi-factor authentication The system must support multi-factor authentication to protect against user impersonation and credential theft.**
☒ P, Q, N or I Notes: P	**4. Risk-based factors The system must support risk-based factors and scores that are based on factors such as, but not limited to, device and location.**
☒ P, Q, N or I Notes: P	**5. Identity lifecycle management components The system must include the following identity lifecycle management components for risk-based critical applications not limited to end users but also for generic accounts and system/service accounts:**
P	1) Identity Creation
P	2) Identity provisioning
P	3) Attribute maps
P	4) Authentication (e.g., password policies and synchronization)

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Active Cyber
DATE: 6/11/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes:P	**6. Security event logging The system must log security information and events.**
	Security Information and Event Management (SIEM) – Splunk
	Cloud Services: Azure, AWS, Oracle, Google
☒ P, Q, N or I Notes:	**7. Security Certifications The system must comply too or have the following security certifications:**
comply	1) NIST 800-53
comply	2) FedRamp
comply	3) HIPAA
comply	4) SOC 2 Type II
	Note:
	IRS require a 45-day letter approval for new cloud solutions.
☒ P, Q, N or I Notes:P	**8. SIEM (Splunk) integration The system must be able to integrate with the State of Maine Security Information and Event Monitoring (SIEM) Splunk for Security Operations Center operations.**
☒ P, Q, N or I Notes:P	**9. Core constituent data. The system must maintain a central repository of basic (core) constituent data, that can be used by any SoM application to reduce data redundancy and outdated or inaccurate information while maintaining confidentiality.**
☒ P, Q, N or I Notes:P	**11. Data Management. The system must apply the Data Management Rules to the constituent profile data as per the SoM Data Management Policies.**
☒ P, Q, N or I Notes:P	**12. SOM Employee. The system must support multiple identities for SOM employees that work with the portal in a support role.**
P	1) SOM Employee identity and credentials for supporting the application.

P	2) Constituent identity and credentials to use the state services offered through the portal.

☒ P, Q, N or I Notes:P	**13. APIs. The system must be able to connect to at least one agency application.**
	Considerations:
	a) OpenID, OAuth, WS-Fed, SAML, LDAP, Active Directory, Application Programming Interfaces (APIs), Software Development
	b) Develop once and reuse often with other agencies would be ideal
☒ P, Q, N or I Notes:P	**14. User identification matching. The system must be able to match the identity of the portal user to the identity of the same user in the agency system.**
☒ P, Q, N or I Notes:P	**15. Single sign-on. The system must support single sign-on to the agency application.**
☒ P, Q, N or I Notes:P	**16. Import user profile data from agency systems. The system must be able to import user data from different SoM applications to ensure offboarding happens in a timely manner, so that government resources are protected from fraud. (example: death records)**
☒ P, Q, N or I Notes:	**17. History logging.** 1) The system must log all actions taken by:
P	a) Constituents
P	b) MaineIT support
P	Including but not limited to:
P	c) who made the change
P	d) when the change was made
P	e) what changed

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Active Cyber
DATE: 6/11/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes:P	**18. Reporting. The logging data (history) must be available for constituent and system dashboards and reporting in general.**
☒ P, Q, N or I Notes:P	**19. Security Controls. The system must comply to the following security controls:**
P	1) DDOS Protections[WN1] ,
P	2) OWASP Top 10
P	a) Cross Site Scripting,
P	b) SQL Injection,
P	3) Authentication bypass,
P	a) poorly authenticated APIs,
P	b) Role based access controls,
P	c) proper session control
P	4) Real-time visibility,
P	5) Anomalous behavior,
P	6) User sign with geo-location tracking,
P	Geo-blocking capabilities.
P	Security controls must include Web Application Firewall [WN1]
☒ P, Q, N or I Notes:P	**20. General System Requirements.** 1) Mobile Support with Native App; (iOS and Android)
P	2) System availability: 24/7 with 4x1-hour outages per year
P	3) Identity relationships must be tracked in the cloud infrastructure.
P	4) Support responsive web and web browsers.
P	a. Supports Windows, Chrome, and Macintosh operating systems
☒ P, Q, N or I Notes:P	**21. Training and Support.** 1) Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Active Cyber
DATE: 6/11/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

P	2) MaineIT will require technical/administrator training. There will be initial training and on-going training as users are added.
P	3) Have a continuous process to ensure constituents that may have run into issues setting up accounts can have help 24/7.
☒ P, Q, N or I Notes:P	**22. Support Requirements** 1) The Bidder will provide support, and maintenance for the solution to begin immediately after receiving the State's official acceptance of the implemented solution.
P	2) Support and maintenance will be provided for the terms and duration specified in the contract.
P	3) The Bidder will address all questions and reported problems related to the technical and functional operation of the system.
Q doesn't say toll free	4) The Bidder must provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours: 8:00 a.m. to 5:00 p.m. Eastern Standard Time.
P	5) As part of the maintenance agreement, the Bidder will make all product releases and upgrades available to the State at no additional charge.
P	6) All release and upgrades shall be implemented and tested by the Bidder, outside of the normal operating hours of the State government.
P	7) User testing shall occur during normal State business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State government.
☒ P, Q, N or I Notes:P	**23. Hosting** Solution can comply with MaineIT remote hosting policies. a) Remote Hosting Policy http://maine.gov/oit/policies/RemoteHostingPolicy.pdf b) Hosting Customization Policy http://maine.gov/oit/policies/HostingCustomizationPolicy.pdf
☒ P, Q, N or I Notes:P	**24. Disaster Recovery** Proposed Solution can comply with MaineIT security requirements and remote hosting requirements, without requiring waivers, before contract finalization.
P	1) Maintaining an availability metric of ninety-nine-point nine percent (99.9%) of uptime

P	2) Ensuring the capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six hours (i.e., maximum data loss cannot exceed six (6) hours);
P	3) Ensuring a recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours;
P	4) Ensuring the hosting environment provides adequate capacity to ensure that, under ethernet connectivity to the client device, data inquiry/lookup response is within three (3) seconds, and data modification response is within five (5) seconds;
Partial weekly zero down time releases	5) Providing the Department at least thirty (30) calendar day advance written notice of any material change in network operations or architecture;
Partial weekly zero down time releases	6) Ensuring any planned material change in network operations or architecture cannot be made without the prior written consent of the Department; and Outlining of all Service Level Agreements (SLAs) for technical support (the awarded Bidder shall be open to negotiation to ensure the SLAs meet the Department’s needs

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

☒1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
P, N, Q, or I & Notes:P

☒1b) Detailed description of the technologies, software and / or hardware for each of the components.
P, N, Q, or I & Notes:P

☒1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Active Cyber
DATE: 6/11/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

P, N, Q, or I & Notes:P

☒1d) Description of the overall platform and architecture of the proposed solution(s).
P, N, Q, or I & Notes:P

☒1e) Description of any third-party software or partnerships required for the proposed Solution(s).
P, N, Q, or I & Notes:P

☒2a) A detailed timeline and description of milestones, deliverables, tasks
P, N, Q, or I & Notes:P

☒2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period
P, N, Q, or I & Notes:Q no resume

☒2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
P, N, Q, or I & Notes:P

☒2d) Average time to market for each component.
P, N, Q, or I & Notes:P

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State’s, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual’s identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. ☒Capture Constituent Identity and profile data.

P, N, Q, or I & Notes:P

b. ☒Provide identity provisioning and deprovisioning.
P, N, Q, or I & Notes:P

c. ☒Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
   i. Identity Creation
   ii. Identity provisioning
   iii. Attribute maps
   iv. Authentication (e.g., password policies and synchronization)
   P, N, Q, or I & Notes:P

d. ☒Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies.
P, N, Q, or I & Notes:P

e. ☒Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
P, N, Q, or I & Notes:P

f. ☐Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.
P, N, Q, or I & Notes:

g. ☒Allow for multiple role selections for the following identities:
   i. Individual
   ii. Business Owner
   iii. Support multiple identities for State employees that work with the portal in a support role:
      (a) SOM Employee identity and credentials for supporting the application.
      (b) Constituent identity and credentials to use the state services offered through the portal.
   iv. Multi role individual (Individual and Business Owner)
   P, N, Q, or I & Notes:P

h. ☒Have the ability to provide levels of proofing which will be directly tied to the Constituent’s level of consent given.
P, N, Q, or I & Notes:P

i. ☒Support multi-factor authentication to protect against user impersonation and credential theft.
P, N, Q, or I & Notes:P

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Active Cyber
DATE: 6/11/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

B.2. ☒The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.
P, N, Q, or I & Notes:P

a. Disclosure and Consent Management

The desire of the State is to be as transparent as possible and respect the privacy of the individual interacting with the Constituents' Portal. Consent is a core tenant of maintaining the public trust in the Constituents' Portal and will be a foundational component of the architecture.

The Disclosure and Consent Management solution shall include:

i. ☒Granular consent management that encompasses the automated functions necessary to create, modify, revoke, and manage Constituent consents.
ii. ☒Allow users the ability to opt-in and opt-out of data sharing and services within the Constituents' portal.
iii. ☒Obtain user consent both in an interactive and set preference mode for a variety of transactions on the Portal.
iv. ☒Support administrative users' management of standard legal disclaimers and data classification for transactions.
v. ☒Highly configurable with version control and history tracking for consent language.
vi. ☒Ability for end user to access a retrievable log of granted consent and data usage on the portal derived from the consent.

P, N, Q, or I & Notes:P

b. Recommendation Technology

The State is seeking options which, while maintaining individual privacy, will collect and analyze data about user interactions, behavior, and preferences. The

expected outcome of this will be to provide insights and intelligence that help the State make informed decisions and improve Constituent experiences.

i. ☒From the user perspective, the portal should be able to make real-time recommendations for related services.
ii. ☒Data captured in this environment must be obfuscated, as to not allow any party to directly target or track the preferences of an individual or their usage of the portal.
iii. ☒Solution providers should discuss in detail their use, storage, destruction of metadata, and tracking technologies with emphasis on how their offering provides analytical insights while protecting the individual user privacy.

P, N, Q, or I & Notes:P

c. Data Management

The State is seeking the ability for the portal's Constituent identity to be linked to records maintained by individual State agencies. The proposed solution will include:

i. ☒Capabilities to streamline the sharing of data between State systems, including
    i. The identity assurance level
    ii. Agency to user notifications
    iii. Verification of user consent
    iv. Identity resolution
    v. Data sharing between agencies.
ii. ☒Maintain a central repository of basic (core) Constituent data, that can be used by any State application to reduce data redundancy, and outdated or inaccurate information while maintaining confidentiality.
iii. ☒Ability to integrate with State applications using, OpenID, OAuth, Web Services Federation Protocol (WS-Fed), Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), Active Directory, Application Programming Interface (API) or equivalent protocols.
iv. ☒Ability to match the identity of the portal user to the identity of the same user in the Agency system.
v. ☒Log all actions taken by:
    i. Constituents
    ii. MaineIT Support, including:
        (a) Who made the change
        (b) When the change was made

(c) What changed to and from

vi. ☒Logging data must be available for system dashboards and reporting.

P, N, Q, or I & Notes:P

d. Customer Service

The State is seeking solution(s) to provide 24/7/365 customer service to Constituents regardless of their location or technical abilities.

- i. ☒Support Constituents with personalized and timely assistance.
- ii. ☒Provide the state options to support our Constituents across multiple channels including, but not limited to phone, email, chat, etc.

P, N, Q, or I & Notes: P

C.1. General System

- a. ☒Mobile support with native app (iOS and Android)
- b. ☒System availability: 24/7 with a maximum of four (4) 1-hour outages per year
- c. ☒Identity relationships must be tracked in the cloud infrastructure.
- d. ☒Support responsive web and web browsers.
  - i. ☒Supports Windows, Chrome, and Macintosh operating systems.

P, N, Q, or I & Notes:P

C.2. ☒Compliance with MaineIT Policies & Standards

- a. Architecture Compliance Policy
- b. System and Services Acquisition Policy and Procedures (SA-1)
- c. Application Deployment Certification Policy
- d. Digital Accessibility Policy
- e. Remote Hosting Policy
- f. Data Exchange Policy
- g. Information Security Policy
- h. Access Control Policy (AC-1)
- i. Access Control Procedures for Users (AC-2)
- j. Risk Assessment Policy and Procedures (RA-1)
- k. Vulnerability Scanning Procedure (RA-5)
- l. Security Assessment and Authorization Policy and Procedures (CA-1)
- m. System and Information Integrity Policy and Procedures (SI-1)

n. Configuration Management Policy (CM-1)
o. Web Standards

P, N, Q, or I & Notes:P

C.3. Support and Maintenance

a. ☒Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State's official acceptance of the implemented solution.
P, N, Q, or I & Notes:P
b. ☒Terms and duration of the support and maintenance will be specified in the contract.
P, N, Q, or I & Notes:P

c. ☒All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
P, N, Q, or I & Notes:P
d. ☒Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
P, N, Q, or I & Notes:P
e. ☒All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
P, N, Q, or I & Notes:P
f. ☒All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
P, N, Q, or I & Notes:P
g. ☒User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
P, N, Q, or I & Notes:P

4. Security

The proposed solutions must provide a robust security system that aligns with the States Security Policies, standards, and Processes, Including:

Comply with or have the following security certifications:

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Active Cyber
DATE: 6/11/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

i. ☒National Institute of Standards and Technology (NIST) 800-53
ii. ☒FedRamp
iii. ☒Health Insurance Portability and Accountability Act (HIPAA)
iv. ☒SOC 2 Type II
v. ☒Comply to the following security controls:
vi. ☒DDOS Protections [WN1]
vii. ☒Open Web Application Security Project (OWASP) Top 10
viii. ☒Cross Site Scripting
ix. ☒Structured Query Language (SQL) Injection
x. ☒Authentication bypass
xi. ☒Poorly authenticated APIs
xii. ☒Role based access controls
xiii. ☒Proper session control
xiv. ☒Real-time visibility
xv. ☒Anomalous behavior
xvi. ☒User sign with geo-location tracking
xvii. ☒Geo-blocking capabilities.
xviii. ☒Web Application Firewall [WN1]
xix. ☒System security must include the following security components:
xx. ☒Account take over protections
xxi. ☒Account sign-in Protections
xxii. ☒Behavior detection and evaluation
xxiii. ☒Adaptive AI Technology
xxiv. ☒Bot Protection; identity visitor behavior through analysis, technical and behavioral data.
xxv. ☒The proposed solution must be able to integrate with the State Security Information and Event Monitoring (SIEM) Splunk. Ability to log security information and events.

P, N, Q, or I & Notes:P

5. Licensing

☒The State is aware that multiple licensing options are available and will be required to support the proposed solution in its entirety. The State seeks bids which will provide the most cost-effective licensing approach. Bidders are required to provide a detail breakdown for the proposed licensing.

P, N, Q, or I & Notes:Q Don't have Appendix I

1. Training and OCM (Organizational Change Management)

a. ☒Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
b. ☒Training must include technical and administrator training, initial and ongoing as users are added.
c. ☒Continuous process to ensure Constituents that may have run into issues setting up accounts have help 24/7.
d. ☒Bidders shall guide the State in OCM engagement for the duration of project planning, transition, and final implementation phase including:
    i. Designing and managing team structures with roles and responsibilities to facilitate automated program delivery, while noting any risks anticipated from the lack of readiness in the organization and staffing.
    ii. Ensure a successful transition for the integration of new processes and technology with stakeholders.
    iii. Organizational readiness assessment

P, N, Q, or I & Notes:P

3. Disaster Recovery

a. ☒Availability of ninety-nine-point nine percent (99.9%) of uptime
b. ☒Capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six (6) hours (i.e., maximum data loss cannot exceed six (6) hours)
c. ☒Recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours.

P, N, Q, or I & Notes:P

4. Feature Enhancements

a. ☒The State is seeking two hundred and fifty (250) hours of time and material for each proposed technology (CIAM), Personalized Dashboard, Disclosure and Consent Management, Data Management, and Recommendation Technology) to allow for specifications and enhancements during the contract period.

P, N, Q, or I & Notes:

5. Project Management

a. ☒The State plans to have its own project manager however, the awarded Bidder must have a project manager that has the primary responsibility for executing the project management tasks associated with the project. The awarded Bidder will:
   i. Work in collaboration with the State's Project Manager
   ii. Align with State Project Management processes and practices.

b. ☒Manage the implementation, executing all activities, tasks, deliverables and resource needs, both state and awarded Bidder.

c. ☒Track project status including managing and tracking all project risks, issues and decisions.

d. ☒Track and report status of deliverables and project status

e. ☒The awarded Bidder will provide their approach for project management and administration services including:
   i. Project Management Methodology
   ii. Project Governance
   iii. Resource Allocation and Schedule Management approach
   iv. Communication Management Approach including status reporting and document repository management.
   v. Risk and Issue Management Methodology
   vi. Change Management Methodology
   vii. Quality Management Methodology

P, N, Q, or I & Notes:P

D. Value Added Options (Other)

☐Bidders shall provide value added optional services to address relevant matters that have not been anticipated in this RFP but contribute to successful implementation of the proposed solutions, as well as any technology or services that will reduce risk to the project's quality and continuity. The value-added technology and services will not be included in the evaluation process but may be added during the contract negotiations.

P, N, Q, or I & Notes:N none listed

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Active Cyber
DATE: 6/11/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Active Cyber
DATE: 06032024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

Section I – Preliminary Information (No points – Eligibility Requirements)

(File #1 App. A, B, C)
☒Done – Pass/Fail by Procurement & RFP Coordinator

Section II Organization Qualifications and Experience

(File #2 – App. D, E + other areas that have no Appendix number but are part of File #2)

1. Overview of the Organization (App. D)

☒Bidders must include three examples of projects which demonstrate their experience and expertise in performing these services as well as highlighting the Bidder's stated qualifications and skills.

Statement of qualifications

☒Client name, contact person, Ph#, email.

Contract history with the state may be considered in rating proposals even if not provided by the bidder.

P, N, Q, or I & Notes:

I – Active Cyber provide contact information; for reference projects 2 out 3 meet all six criteria, all projects have contact information marked "Provided upon down selection"

2. Subcontractors (App. E)

☒If subcontractors are to be used, Bidders must provide the name, address, phone number, contact person, and a brief description of the subcontractors' organizational capacity and qualifications.
Business name, contact person, address, ph#, email.
P, N, Q, or I & Notes:
P – no subcontractors

3. Organizational Chart (No Appendix)

☒Bidders must provide an organizational chart. The organizational chart must include the project being proposed. Each position must be identified by position title and corresponding to the personnel job descriptions.
P, N, Q, or I & Notes:
N-Only high level structure, no formal org chart

4. Litigation (No App.)

☒Bidders must attach a list of all current litigation in which the Bidder is named and a list of all closed cases that have closed within the past five (5) years in which the Bidder paid the claimant either as part of a settlement or by decree. For each, list the entity bringing suit, the complaint, the accusation, amount, and outcome.

P, N, Q, or I & Notes:

P – No Attachment

5. Financial Viability (No App.)

☒Bidders must provide a current copy of their Dun & Bradstreet Business Information Report Snapshot.

P, N, Q, or I - Notes:

N – No Attachment

6. Licensure/Certification (No App.)

☒Bidders *may* provide documentation of any applicable licensure/certification or specific credentials that are related to providing the proposed services of the RFP.

P, N, Q, or I & Notes:

N- was not included

7. Certificate of Insurance (No App.)

☒Bidders must provide a certificate of insurance on a standard ACORD form (or the equivalent) evidencing the Bidder's general liability, professional liability and any other relevant liability insurance policies that might be associated with the proposed services.

P, N, Q, or I & Notes:

N – no attachment

Section III - Proposed Services

(File #3 – App. F, G, H)

1. Technical Assessment (App. F)

☒Done

2. Services to be Provided (App. G)

Note: on App. G Detailed Technical and Functional Requirements Excel spreadsheet, a tab is labeled User Stories. No response is required for Tab 3; these were provided to bidders for clarity and understanding of the expected journey a Constituent will experience.

☒ **P**, Q, N or I Notes:	**1. System security components System security must include the following security components:**
	1) Account Take Over Protections
	a) Account Sign-in Protections
	a) Account Sign-in Protections
	a) Adaptive AI Technology
	b) Bot Protection: identify visitor behavior through analysis of technical and behavioral data.
☒ P, Q, N or **I** Notes: All features are an add on and not native	**2. Identity Proofing must have the ability to provide levels of proofing which will be directly tied to the constituent's level of access.**
	1) Define various levels of id proofing
	2) Document Image Capture
	3) Close coupling with authentication
☒ **P**, Q, N or I Notes:	**3. Multi-factor authentication The system must support multi-factor authentication to protect against user impersonation and credential theft.**
☒ **P**, Q, N or I Notes:	**4. Risk-based factors The system must support risk-based factors and scores that are based on factors such as, but not limited to, device and location.**
☒ **P**, Q, N or I Notes:	**5. Identity lifecycle management components The system must include the following identity lifecycle management components for risk-based critical applications not limited to end users but also for generic accounts and system/service accounts:**
	1) Identity Creation
	2) Identity provisioning

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Active Cyber
DATE: 06032024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

	3) Attribute maps
	4) Authentication (e.g., password policies and synchronization)

☒ P, Q, **N** or I Notes: Doesn't go into detail around aws logs; no Id.ME	**6. Security event logging The system must log security information and events.**
	Security Information and Event Management (SIEM) – Splunk
	Cloud Services: Azure, **AWS**, Oracle, Google
☒ P, Q, **N** or I Notes:	**7. Security Certifications The system must comply too or have the following security certifications:**
Answers only for Okta, nothing about ID.me	1) NIST 800-53
	2) FedRamp
	3) HIPAA
	4) SOC 2 Type II
	Note:
	IRS require a 45-day letter approval for new cloud solutions.
☒ **P**, Q, N or I	**8. SIEM (Splunk) integration The system must be able to integrate with the State of Maine Security Information and Event Monitoring (SIEM) Splunk for Security Operations Center operations.**

Notes:	
☒ P, **Q**, N or **I** Notes: How does this work with external constituent data?	9. **Core constituent data. The system must maintain a central repository of basic (core) constituent data, that can be used by any SoM application to reduce data redundancy and outdated or inaccurate information while maintaining confidentiality.**
☒ P, Q, N or **I** Notes:	11. **Data Management. The system must apply the Data Management Rules to the constituent profile data as per the SoM Data Management Policies.**
☒ P, **Q**, N or I Notes:	12. **SOM Employee. The system must support multiple identities for SOM employees that work with the portal in a support role.**
No mention of Id.Me	1) SOM Employee identity and credentials for supporting the application.
	2) Constituent identity and credentials to use the state services offered through the portal.

☒ P, Q, N or **I** Notes:	13. **APIs. The system must be able to connect to at least one agency application.**
	Considerations:
	a) OpenID, OAuth, WS-Fed, SAML, LDAP, Active Directory, Application Programming Interfaces (APIs), Software Development
	b) Develop once and reuse often with other agencies would be ideal

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Active Cyber
DATE: 06032024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

☐ P, **Q**, N or I Notes: Is this going to cause unmanageable dub accounts	**14. User identification matching. The system must be able to match the identity of the portal user to the identity of the same user in the agency system.**
☒ **P**, Q, N or I Notes:	**15. Single sign-on. The system must support single sign-on to the agency application.**
☒ P, Q, N or **I** Notes:	**16. Import user profile data from agency systems. The system must be able to import user data from different SoM applications to ensure offboarding happens in a timely manner, so that government resources are protected from fraud. (example: death records)**
☒ P, Q, **N** or I Notes:	**17. History logging.** 1) The system must log all actions taken by:
No id.me info	a) Constituents
	b) MaineIT support
	Including but not limited to:
	c) who made the change
	d) when the change was made
	e) what changed
☒ P, Q, **N** or I Notes: no ID.me info	**18. Reporting. The logging data (history) must be available for constituent and system dashboards and reporting in general.**
☒ P, Q, **N** or I Notes:	**19. Security Controls. The system must comply to the following security controls:**
No mention of ID.me	1) DDOS Protections[WN1] ,
	2) OWASP Top 10
	a) Cross Site Scripting,
	b) SQL Injection,

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Active Cyber
DATE: 06032024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

	3) Authentication bypass,
	a) poorly authenticated APIs,
	b) Role based access controls,
	c) proper session control
	4) Real-time visibility,
	5) Anomalous behavior,
	6) User sign with geo-location tracking,
	Geo-blocking capabilities.
	Security controls must include Web Application Firewall [WN1]
☒ P, Q, **N** or I Notes:	**20. General System Requirements.** 1) Mobile Support with Native App; (iOS and Android)
No mention of ID.me	2) System availability: 24/7 with 4x1-hour outages per year
	3) Identity relationships must be tracked in the cloud infrastructure.
	4) Support responsive web and web browsers.
	a. Supports Windows, Chrome, and Macintosh operating systems
☒ P, Q, **N** or I Notes:	**21. Training and Support.** 1) Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
Does not talk to detailed program or training for ID.me	2) MaineIT will require technical/administrator training. There will be initial training and on-going training as users are added.
	3) Have a continuous process to ensure constituents that may have run into issues setting up accounts can have help 24/7.
☒ P, Q, **N** or I Notes:	**22. Support Requirements** 1) The Bidder will provide support, and maintenance for the solution to begin immediately after receiving the State's official acceptance of the implemented solution.
No ID.me	2) Support and maintenance will be provided for the terms and duration specified in the contract.

	3) The Bidder will address all questions and reported problems related to the technical and functional operation of the system.
	4) The Bidder must provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours: 8:00 a.m. to 5:00 p.m. Eastern Standard Time.
	5) As part of the maintenance agreement, the Bidder will make all product releases and upgrades available to the State at no additional charge.
	6) All release and upgrades shall be implemented and tested by the Bidder, outside of the normal operating hours of the State government.
	7) User testing shall occur during normal State business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State government.
☒ P, Q, **N** or I Notes: No id.me	**23. Hosting** Solution can comply with MaineIT remote hosting policies. a) Remote Hosting Policy http://maine.gov/oit/policies/RemoteHostingPolicy.pdf b) Hosting Customization Policy http://maine.gov/oit/policies/HostingCustomizationPolicy.pdf
☒ P, Q, N or **I** Notes:	**24. Disaster Recovery** Proposed Solution can comply with MaineIT security requirements and remote hosting requirements, without requiring waivers, before contract finalization.
Mostly relevant to Okta, but missing ID.me information	1) Maintaining an availability metric of ninety-nine-point nine percent (99.9%) of uptime
	2) Ensuring the capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six hours (i.e., maximum data loss cannot exceed six (6) hours);
	3) Ensuring a recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours;

	4) Ensuring the hosting environment provides adequate capacity to ensure that, under ethernet connectivity to the client device, data inquiry/lookup response is within three (3) seconds, and data modification response is within five (5) seconds;
	5) Providing the Department at least thirty (30) calendar day advance written notice of any material change in network operations or architecture;
	6) Ensuring any planned material change in network operations or architecture cannot be made without the prior written consent of the Department; and Outlining of all Service Level Agreements (SLAs) for technical support (the awarded Bidder shall be open to negotiation to ensure the SLAs meet the Department's needs

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

☒1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
P, **N**, Q, or I & Notes:
Only talked technology, did not included any of SoM goals or additional requirements around dashboarding

☒1b) Detailed description of the technologies, software and / or hardware for each of the components.
P, **N**, Q, or I & Notes:
Very high level does not go into the aws infrastructure until later in rfp

☒1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.
P, **N**, Q, or I & Notes:
Idme requires add-ons but they don't talk about out of box features

☒1d) Description of the overall platform and architecture of the proposed solution(s).
P, **N**, Q, or I & Notes:
Does not talk about the underlying aws architecture

☒1e) Description of any third-party software or partnerships required for the proposed Solution(s).
P, N, Q, or **I** & Notes:

☒2a) A detailed timeline and description of milestones, deliverables, tasks
P, N, Q, or **I** & Notes:

☒2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period
P, **N**, Q, or I & Notes:
No resumes or actual people identified, just people

☒2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
P, N, Q, or **I** & Notes:

☐2d) Average time to market for each component.
P, N, Q, or **I** & Notes:

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. ☒Capture Constituent Identity and profile data.
   P, N, Q, or I & Notes:
b. ☒Provide identity provisioning and deprovisioning.
   P, N, Q, or I & Notes:
c. ☒Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:

    i. Identity Creation
    ii. Identity provisioning
    iii. Attribute maps
    iv. Authentication (e.g., password policies and synchronization)
    P, N, Q, or I & Notes:

d. ☒Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies.
P, **N**, Q, or I & Notes: doesn't talk about

e. ☒Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
P, N, Q, or I & Notes:

f. ☒Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.
P, N, **Q**, or I & Notes: more detail would be nice

g. ☒Allow for multiple role selections for the following identities:
    i. Individual
    ii. Business Owner
    iii. Support multiple identities for State employees that work with the portal in a support role:
        (a) SOM Employee identity and credentials for supporting the application.
        (b) Constituent identity and credentials to use the state services offered through the portal.
    iv. Multi role individual (Individual and Business Owner)
    P, N, **Q**, or I & Notes: does this meet the individual vs Business owner need

h. ☒Have the ability to provide levels of proofing which will be directly tied to the Constituent's level of consent given.
P, **N**, Q, or I & Notes: does not provide idme detail

i. ☒Support multi-factor authentication to protect against user impersonation and credential theft.
P, N, Q, or **I** & Notes:

B.2. ☐The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the

Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.
P, N, Q, or **I** & Notes:

a. Disclosure and Consent Management

The desire of the State is to be as transparent as possible and respect the privacy of the individual interacting with the Constituents' Portal. Consent is a core tenant of maintaining the public trust in the Constituents' Portal and will be a foundational component of the architecture.

The Disclosure and Consent Management solution shall include:

- i. ☐Granular consent management that encompasses the automated functions necessary to create, modify, revoke, and manage Constituent consents.
- ii. ☐Allow users the ability to opt-in and opt-out of data sharing and services within the Constituents' portal.
- iii. ☐Obtain user consent both in an interactive and set preference mode for a variety of transactions on the Portal.
- iv. ☐Support administrative users' management of standard legal disclaimers and data classification for transactions.
- v. ☐Highly configurable with version control and history tracking for consent language.
- vi. ☐Ability for end user to access a retrievable log of granted consent and data usage on the portal derived from the consent.

P, N, Q, or **I** & Notes: talks to "the system" but does not talk to which technology does what

b. Recommendation Technology

The State is seeking options which, while maintaining individual privacy, will collect and analyze data about user interactions, behavior, and preferences. The expected outcome of this will be to provide insights and intelligence that help the State make informed decisions and improve Constituent experiences.

- i. ☒From the user perspective, the portal should be able to make real-time recommendations for related services.

ii. ☒Data captured in this environment must be obfuscated, as to not allow any party to directly target or track the preferences of an individual or their usage of the portal.
iii. ☒Solution providers should discuss in detail their use, storage, destruction of metadata, and tracking technologies with emphasis on how their offering provides analytical insights while protecting the individual user privacy.

P, N, Q, or I & Notes:

c. Data Management

The State is seeking the ability for the portal's Constituent identity to be linked to records maintained by individual State agencies. The proposed solution will include:

i. ☒Capabilities to streamline the sharing of data between State systems, including
    i. The identity assurance level
    ii. Agency to user notifications
    iii. Verification of user consent
    iv. Identity resolution
    v. Data sharing between agencies.
ii. ☒Maintain a central repository of basic (core) Constituent data, that can be used by any State application to reduce data redundancy, and outdated or inaccurate information while maintaining confidentiality.
iii. ☒Ability to integrate with State applications using, OpenID, OAuth, Web Services Federation Protocol (WS-Fed), Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), Active Directory, Application Programming Interface (API) or equivalent protocols.
iv. ☐Ability to match the identity of the portal user to the identity of the same user in the Agency system.
v. ☒Log all actions taken by:
    i. Constituents
    ii. MaineIT Support, including:
        (a) Who made the change
        (b) When the change was made
        (c) What changed to and from
vi. ☐Logging data must be available for system dashboards and reporting.

P, N, **Q**, or I & Notes: the user matching seems like it will just create additional accounts

d. Customer Service

The State is seeking solution(s) to provide 24/7/365 customer service to Constituents regardless of their location or technical abilities.

i. ☒Support Constituents with personalized and timely assistance.
ii. ☒Provide the state options to support our Constituents across multiple channels including, but not limited to phone, email, chat, etc.

P, N, Q, or **I** & Notes:

C.1. General System

a. ☒Mobile support with native app (iOS and Android)
b. ☒System availability: 24/7 with a maximum of four (4) 1-hour outages per year
c. ☒Identity relationships must be tracked in the cloud infrastructure.
d. ☒Support responsive web and web browsers.
  i. ☒Supports Windows, Chrome, and Macintosh operating systems.

P, N, Q, or I & Notes:

C.2. ☒Compliance with MaineIT Policies & Standards

a. Architecture Compliance Policy
b. System and Services Acquisition Policy and Procedures (SA-1)
c. Application Deployment Certification Policy
d. Digital Accessibility Policy
e. Remote Hosting Policy
f. Data Exchange Policy
g. Information Security Policy
h. Access Control Policy (AC-1)
i. Access Control Procedures for Users (AC-2)
j. Risk Assessment Policy and Procedures (RA-1)
k. Vulnerability Scanning Procedure (RA-5)
l. Security Assessment and Authorization Policy and Procedures (CA-1)
m. System and Information Integrity Policy and Procedures (SI-1)
n. Configuration Management Policy (CM-1)
o. Web Standards

P, N, Q, or **I** & Notes:
Weak responses, however in app F they do state they can meet all requirements

C.3. Support and Maintenance

a. ☒Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State's official acceptance of the implemented solution.
P, **N**, Q, or I & Notes: first mention of "dedicated support partner" but no other information

b. ☒Terms and duration of the support and maintenance will be specified in the contract.
P, N, Q, or I & Notes:

c. ☒All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
P, **N**, Q, or I & Notes: does not state

d. ☒Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
P, N, **Q**, or I & Notes: does that number include idme

e. ☒All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
P, N, **Q**, or I & Notes: what about idme

f. ☒All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
P, N, Q, or **I** & Notes: noted – upgrades are non impactful

g. ☒User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
P, N, Q, or **I** & Notes:

4. Security

The proposed solutions must provide a robust security system that aligns with the States Security Policies, standards, and Processes, Including:

Comply with or have the following security certifications:

i. ☒National Institute of Standards and Technology (NIST) 800-53

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Active Cyber
DATE: 06032024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

ii. ☒FedRamp
iii. ☒Health Insurance Portability and Accountability Act (HIPAA)
iv. ☒SOC 2 Type II
v. ☒Comply to the following security controls:
vi. ☒DDOS Protections [WN1]
vii. ☒Open Web Application Security Project (OWASP) Top 10
viii. ☒Cross Site Scripting
ix. ☒Structured Query Language (SQL) Injection
x. ☒Authentication bypass
xi. ☒Poorly authenticated APIs
xii. ☒Role based access controls
xiii. ☒Proper session control
xiv. ☒Real-time visibility
xv. ☒Anomalous behavior
xvi. ☒User sign with geo-location tracking
xvii. ☒Geo-blocking capabilities.
xviii. ☒Web Application Firewall [WN1]
xix. ☒System security must include the following security components:
xx. ☒Account take over protections
xxi. ☒Account sign-in Protections
xxii. ☒Behavior detection and evaluation
xxiii. ☒Adaptive AI Technology
xxiv. ☒Bot Protection; identity visitor behavior through analysis, technical and behavioral data.
xxv. ☒The proposed solution must be able to integrate with the State Security Information and Event Monitoring (SIEM) Splunk. Ability to log security information and events.

P, **N**, Q, or I & Notes:
only talks to okta and no idme

5. Licensing

☒The State is aware that multiple licensing options are available and will be required to support the proposed solution in its entirety. The State seeks bids which will provide the most cost-effective licensing approach. Bidders are required to provide a detail breakdown for the proposed licensing.

P, **N**, Q, or I & Notes: attachment was not included with bid

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Active Cyber
DATE: 06032024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

1. **Training and OCM (Organizational Change Management)**
   a. ☒Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
   b. ☒Training must include technical and administrator training, initial and ongoing as users are added.
   c. ☒Continuous process to ensure Constituents that may have run into issues setting up accounts have help 24/7.
   d. ☒Bidders shall guide the State in OCM engagement for the duration of project planning, transition, and final implementation phase including:
      i. Designing and managing team structures with roles and responsibilities to facilitate automated program delivery, while noting any risks anticipated from the lack of readiness in the organization and staffing.
      ii. Ensure a successful transition for the integration of new processes and technology with stakeholders.
      iii. Organizational readiness assessment

P, N, Q, or **I** & Notes:

3. **Disaster Recovery**
   a. ☒Availability of ninety-nine-point nine percent (99.9%) of uptime
   b. ☒Capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six (6) hours (i.e., maximum data loss cannot exceed six (6) hours)
   c. ☐Recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours.

P, **N**, Q, or I & Notes: does not meet rto or talk to idme

4. **Feature Enhancements**

a. ☒The State is seeking two hundred and fifty (250) hours of time and material for each proposed technology (CIAM), Personalized Dashboard, Disclosure and Consent Management, Data Management, and Recommendation Technology) to allow for specifications and enhancements during the contract period.

P, N, Q, or I & Notes:

5. Project Management

a. ☒The State plans to have its own project manager however, the awarded Bidder must have a project manager that has the primary responsibility for executing the project management tasks associated with the project. The awarded Bidder will:
   i. Work in collaboration with the State's Project Manager
   ii. Align with State Project Management processes and practices.
b. ☒Manage the implementation, executing all activities, tasks, deliverables and resource needs, both state and awarded Bidder.
c. ☒Track project status including managing and tracking all project risks, issues and decisions.
d. ☒Track and report status of deliverables and project status
e. ☒The awarded Bidder will provide their approach for project management and administration services including:
   i. Project Management Methodology
   ii. Project Governance
   iii. Resource Allocation and Schedule Management approach
   iv. Communication Management Approach including status reporting and document repository management.
   v. Risk and Issue Management Methodology
   vi. Change Management Methodology
   vii. Quality Management Methodology

P, N, Q, or **I** & Notes:

D. Value Added Options (Other)

☐Bidders shall provide value added optional services to address relevant matters that have not been anticipated in this RFP but contribute to successful implementation of the proposed solutions, as well as any technology or services that will reduce risk to the project's quality and continuity. The value-added technology and services will not be included in the evaluation process but may be added during the contract negotiations.

P, **N**, Q, or I & Notes:

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Active Cyber
DATE: 06032024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

Would have liked more detail on the phone support mentioned as well as the “add ons” for id.me under app G

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Active Cyber
DATE: 04 Jun 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: MaineIT

Section I – Preliminary Information (No points – Eligibility Requirements)

(File #1 App. A, B, C)
☒Done – Pass/Fail by Procurement & RFP Coordinator

Section II Organization Qualifications and Experience

(File #2 – App. D, E + other areas that have no Appendix number but are part of File #2)

1. **Overview of the Organization (App. D)**
   ☒Bidders must include three examples of projects which demonstrate their experience and expertise in performing these services as well as highlighting the Bidder's stated qualifications and skills.
   N: Weak response

   Statement of qualifications
   ☒Client name, contact person, Ph#, email.
   Contract history with the state may be considered in rating proposals even if not provided by the bidder.
   N: Contact details NOT provided.
   N: Scope & details of projects NOT provided.

2. **Subcontractors (App. E)**
   ☐If subcontractors are to be used, Bidders must provide the name, address, phone number, contact person, and a brief description of the subcontractors' organizational capacity and qualifications.
   Business name, contact person, address, ph#, email.
   N: NO response

3. **Organizational Chart (No Appendix)**
   ☐Bidders must provide an organizational chart. The organizational chart must include the project being proposed. Each position must be identified by position title and corresponding to the personnel job descriptions.
   N: NO response

4. **Litigation (No App.)**
   ☐Bidders must attach a list of all current litigation in which the Bidder is named and a list of all closed cases that have closed within the past five (5) years in which the

Bidder paid the claimant either as part of a settlement or by decree. For each, list the entity bringing suit, the complaint, the accusation, amount, and outcome.

N: NO response

5. **Financial Viability (No App.)**
☐Bidders must provide a current copy of their Dun & Bradstreet Business Information Report Snapshot.

N: NO response

6. **Licensure/Certification (No App.)**
☐Bidders *may* provide documentation of any applicable licensure/certification or specific credentials that are related to providing the proposed services of the RFP.

N: NO response

7. **Certificate of Insurance (No App.)**
☐Bidders must provide a certificate of insurance on a standard ACORD form (or the equivalent) evidencing the Bidder's general liability, professional liability and any other relevant liability insurance policies that might be associated with the proposed services.

N: NO response

Section III - Proposed Services

(File #3 – App. F, G, H)

1. **Technical Assessment (App. F)**
☒Done

2. **Services to be Provided (App. G)**

Note: on App. G Detailed Technical and Functional Requirements Excel spreadsheet, a tab is labeled User Stories. No response is required for Tab 3; these were provided to bidders for clarity and understanding of the expected journey a Constituent will experience.

☒ *P: Strong response*	**1. System security components System security must include the following security components:**
	1) Account Take Over Protections
	a) Account Sign-in Protections
	a) Account Sign-in Protections

	a) Adaptive AI Technology
	b) Bot Protection: identify visitor behavior through analysis of technical and behavioral data.
☒ *P: Strong response*	**2. Identity Proofing must have the ability to provide levels of proofing which will be directly tied to the constituent's level of access.**
	1) Define various levels of id proofing
	2) Document Image Capture
	3) Close coupling with authentication
☒ *P: Strong response*	**3. Multi-factor authentication The system must support multi-factor authentication to protect against user impersonation and credential theft.**
☒ *P: Strong response*	**4. Risk-based factors The system must support risk-based factors and scores that are based on factors such as, but not limited to, device and location.**
☒ *P: Strong response*	**5. Identity lifecycle management components The system must include the following identity lifecycle management components for risk-based critical applications not limited to end users but also for generic accounts and system/service accounts:**
	1) Identity Creation
	2) Identity provisioning
	3) Attribute maps
	4) Authentication (e.g., password policies and synchronization)
☒ *N: Weak response. Covers Okta, but NOT ID.me.*	**6. Security event logging The system must log security information and events.**
	Security Information and Event Management (SIEM) – Splunk
	Cloud Services: Azure, AWS, Oracle, Google

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Active Cyber
DATE: 04 Jun 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: MaineIT

☒ *N: Weak response. Covers Okta, but NOT ID.me.* *N: NO ack of the IRS 45-day notice.*	**7. Security Certifications The system must comply too or have the following security certifications:**
	1) NIST 800-53
	2) FedRamp
	3) HIPAA
	4) SOC 2 Type II
	Note:
	IRS require a 45-day letter approval for new cloud solutions.
☒ *N: Weak response. Covers Okta, but NOT ID.me*	**8. SIEM (Splunk) integration The system must be able to integrate with the State of Maine Security Information and Event Monitoring (SIEM) Splunk for Security Operations Center operations.**
☒ *N: Weak response. Covers Okta, but NOT ID.me*	**9. Core constituent data. The system must maintain a central repository of basic (core) constituent data, that can be used by any SoM application to reduce data redundancy and outdated or inaccurate information while maintaining confidentiality.**
☒ *N: Weak response* *N: Partial, but NO explanation* *N: Covers Okta, but NOT ID.me*	**11. Data Management. The system must apply the Data Management Rules to the constituent profile data as per the SoM Data Management Policies.**

☒ *P: Strong response*	**12. SOM Employee. The system must support multiple identities for SOM employees that work with the portal in a support role.**
	1) SOM Employee identity and credentials for supporting the application.
	2) Constituent identity and credentials to use the state services offered through the portal.
☒ *P: Strong response*	**13. APIs. The system must be able to connect to at least one agency application.**
	Considerations:
	a) OpenID, OAuth, WS-Fed, SAML, LDAP, Active Directory, Application Programming Interfaces (APIs), Software Development
	b) Develop once and reuse often with other agencies would be ideal
☒ *P: Strong response*	**14. User identification matching. The system must be able to match the identity of the portal user to the identity of the same user in the agency system.**
☒ *P: Strong response*	**15. Single sign-on. The system must support single sign-on to the agency application.**
☒ *P: Strong response*	**16. Import user profile data from agency systems. The system must be able to import user data from different SoM applications to ensure offboarding happens in a timely manner, so that government resources are protected from fraud. (example: death records)**
☒ *N: Weak response. Covers Okta, but NOT ID.me.*	**17. History logging.** 1) The system must log all actions taken by:
	a) Constituents
	b) MaineIT support
	Including but not limited to:

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Active Cyber
DATE: 04 Jun 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: MaineIT

	c) who made the change
	d) when the change was made
	e) what changed
☒ *N: Weak response. Covers Okta, but NOT ID.me.*	**18. Reporting. The logging data (history) must be available for constituent and system dashboards and reporting in general.**
☒ *N: Weak response. Covers Okta, but NOT ID.me.*	**19. Security Controls. The system must comply to the following security controls:**
	1) DDOS Protections[WN1] ,
	2) OWASP Top 10
	a) Cross Site Scripting,
	b) SQL Injection,
	3) Authentication bypass,
	a) poorly authenticated APIs,
	b) Role based access controls,
	c) proper session control
	4) Real-time visibility,
	5) Anomalous behavior,
	6) User sign with geo-location tracking,
	Geo-blocking capabilities.
	Security controls must include Web Application Firewall [WN1]
☒ *N: Weak response. Covers Okta, but NOT ID.me.*	**20. General System Requirements.** 1) Mobile Support with Native App; (iOS and Android)
	2) System availability: 24/7 with 4x1-hour outages per year

	3) Identity relationships must be tracked in the cloud infrastructure.
	4) Support responsive web and web browsers.
	a. Supports Windows, Chrome, and Macintosh operating systems
☒ *N: Weak response. Covers Okta, but NOT ID.me.*	**21. Training and Support.** 1) Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
	2) MaineIT will require technical/administrator training. There will be initial training and on-going training as users are added.
	3) Have a continuous process to ensure constituents that may have run into issues setting up accounts can have help 24/7.
☒ *N: Weak response. Covers Okta, but NOT ID.me.*	**22. Support Requirements** 1) The Bidder will provide support, and maintenance for the solution to begin immediately after receiving the State's official acceptance of the implemented solution.
	2) Support and maintenance will be provided for the terms and duration specified in the contract.
	3) The Bidder will address all questions and reported problems related to the technical and functional operation of the system.
	4) The Bidder must provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours: 8:00 a.m. to 5:00 p.m. Eastern Standard Time.
	5) As part of the maintenance agreement, the Bidder will make all product releases and upgrades available to the State at no additional charge.
	6) All release and upgrades shall be implemented and tested by the Bidder, outside of the normal operating hours of the State government.

	7) User testing shall occur during normal State business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State government.
☒ *N: Weak response. Covers Okta, but NOT ID.me.*	**23. Hosting** Solution can comply with MaineIT remote hosting policies. a) Remote Hosting Policy http://maine.gov/oit/policies/RemoteHostingPolicy.pdf b) Hosting Customization Policy http://maine.gov/oit/policies/HostingCustomizationPolicy.pdf
☒ *N: Weak response. Covers Okta, but NOT ID.me.*	**24. Disaster Recovery** Proposed Solution can comply with MaineIT security requirements and remote hosting requirements, without requiring waivers, before contract finalization.
	1) Maintaining an availability metric of ninety-nine-point nine percent (99.9%) of uptime
	2) Ensuring the capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six hours (i.e., maximum data loss cannot exceed six (6) hours);
	3) Ensuring a recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours;
	4) Ensuring the hosting environment provides adequate capacity to ensure that, under ethernet connectivity to the client device, data inquiry/lookup response is within three (3) seconds, and data modification response is within five (5) seconds;
	5) Providing the Department at least thirty (30) calendar day advance written notice of any material change in network operations or architecture;
	6) Ensuring any planned material change in network operations or architecture cannot be made without the prior written consent of the Department; and Outlining of all Service Level Agreements (SLAs) for technical support (the awarded Bidder shall be open to negotiation to ensure the SLAs meet the Department's needs

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Active Cyber
DATE: 04 Jun 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: MaineIT

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

☒1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
P: Strong response

☒1b) Detailed description of the technologies, software and / or hardware for each of the components.
P: Strong response

☒1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.
P: Strong response

☒1d) Description of the overall platform and architecture of the proposed solution(s).
P: Strong response

☒1e) Description of any third-party software or partnerships required for the proposed Solution(s).
P: Adequate response
N: No mention of CarahSoft.

☒2a) A detailed timeline and description of milestones, deliverables, tasks
P: Adequate response

☒2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period
N: No resumes
P: Adequate roles & responsibilities

☒2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
N: Not detailed enough to ascertain viability

☒2d) Average time to market for each component.
N: No mention of ID.me

N: Even the Okta response is generic, and NOT related to this RFP response

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. ☒Capture Constituent Identity and profile data.
P: Strong response

b. ☒Provide identity provisioning and deprovisioning.
P: Strong response

c. ☒Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
   i. Identity Creation
   ii. Identity provisioning
   iii. Attribute maps
   iv. Authentication (e.g., password policies and synchronization)
   P: Strong response

d. ☒Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies.
P: Strong response

e. ☒Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
P: Adequate response

f. ☒Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.
P: Strong response

g. ☒Allow for multiple role selections for the following identities:
   i. Individual
   ii. Business Owner

iii. Support multiple identities for State employees that work with the portal in a support role:
    (a) SOM Employee identity and credentials for supporting the application.
    (b) Constituent identity and credentials to use the state services offered through the portal.

iv. Multi role individual (Individual and Business Owner)
P: Strong response

h. ☒Have the ability to provide levels of proofing which will be directly tied to the Constituent's level of consent given.
N: Irrelevant response

i. ☒Support multi-factor authentication to protect against user impersonation and credential theft.
P: Strong response

B.2. ☒The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.
P: Adequate response

a. Disclosure and Consent Management
The desire of the State is to be as transparent as possible and respect the privacy of the individual interacting with the Constituents' Portal. Consent is a core tenant of maintaining the public trust in the Constituents' Portal and will be a foundational component of the architecture.
The Disclosure and Consent Management solution shall include:

i. ☒Granular consent management that encompasses the automated functions necessary to create, modify, revoke, and manage Constituent consents.
P: Adequate response

ii. ☒Allow users the ability to opt-in and opt-out of data sharing and services within the Constituents' portal.
P: Strong response

iii. ☒Obtain user consent both in an interactive and set preference mode for a variety of transactions on the Portal.
P: Strong response

iv. ☒Support administrative users' management of standard legal disclaimers and data classification for transactions.
P: Strong response

v. ☒Highly configurable with version control and history tracking for consent language.
P: Strong response

vi. ☒Ability for end user to access a retrievable log of granted consent and data usage on the portal derived from the consent.
P: Strong response

b. Recommendation Technology

The State is seeking options which, while maintaining individual privacy, will collect and analyze data about user interactions, behavior, and preferences. The expected outcome of this will be to provide insights and intelligence that help the State make informed decisions and improve Constituent experiences.

i. ☒From the user perspective, the portal should be able to make real-time recommendations for related services.
P: Strong response

ii. ☒Data captured in this environment must be obfuscated, as to not allow any party to directly target or track the preferences of an individual or their usage of the portal.
P: Strong response

iii. ☒Solution providers should discuss in detail their use, storage, destruction of metadata, and tracking technologies with emphasis on how their offering provides analytical insights while protecting the individual user privacy.
P: Strong response

c. Data Management

The State is seeking the ability for the portal's Constituent identity to be linked to records maintained by individual State agencies. The proposed solution will include:

i. ☒Capabilities to streamline the sharing of data between State systems, including
  i. The identity assurance level
  ii. Agency to user notifications
  iii. Verification of user consent
  iv. Identity resolution
  v. Data sharing between agencies.
  P: Strong response

ii. ☒Maintain a central repository of basic (core) Constituent data, that can be used by any State application to reduce data redundancy, and outdated or inaccurate information while maintaining confidentiality.
P: Strong response

iii. ☒Ability to integrate with State applications using, OpenID, OAuth, Web Services Federation Protocol (WS-Fed), Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), Active Directory, Application Programming Interface (API) or equivalent protocols.
P: Strong response

iv. ☒Ability to match the identity of the portal user to the identity of the same user in the Agency system.
P: Strong response

v. ☒Log all actions taken by:
  i. Constituents
  ii. MaineIT Support, including:
    (a) Who made the change
    (b) When the change was made
    (c) What changed to and from
    N: Weak response. Covers Okta, but NOT ID.me.

vi. ☒Logging data must be available for system dashboards and reporting.
N: Weak response. Covers Okta, but NOT ID.me.

d. Customer Service

The State is seeking solution(s) to provide 24/7/365 customer service to Constituents regardless of their location or technical abilities.

  i. ☒Support Constituents with personalized and timely assistance.
  ii. ☒Provide the state options to support our Constituents across multiple channels including, but not limited to phone, email, chat, etc.

Q: "Deploy a sophisticated chatbot": Which product? Was it included in the Cost Proposal?

Q: 24/7 Phone Support: By whom? Was it included in the Cost Proposal?

C.1. General System

a. ☒Mobile support with native app (iOS and Android)
b. ☒System availability: 24/7 with a maximum of four (4) 1-hour outages per year
c. ☒Identity relationships must be tracked in the cloud infrastructure.
d. ☒Support responsive web and web browsers.
  i. ☒Supports Windows, Chrome, and Macintosh operating systems.

N: Weak response. Covers Okta, but NOT ID.me.

C.2. ☒Compliance with MaineIT Policies & Standards

a. Architecture Compliance Policy
b. System and Services Acquisition Policy and Procedures (SA-1)
c. Application Deployment Certification Policy
d. Digital Accessibility Policy
e. Remote Hosting Policy
f. Data Exchange Policy
g. Information Security Policy
h. Access Control Policy (AC-1)
i. Access Control Procedures for Users (AC-2)
j. Risk Assessment Policy and Procedures (RA-1)
k. Vulnerability Scanning Procedure (RA-5)
l. Security Assessment and Authorization Policy and Procedures (CA-1)
m. System and Information Integrity Policy and Procedures (SI-1)
n. Configuration Management Policy (CM-1)
o. Web Standards

N: Does NOT cover Digital Accessibility
N: Does NOT cover Web Standards
P: Otherwise, Strong response

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Active Cyber
DATE: 04 Jun 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: MaineIT

C.3. Support and Maintenance

a. ☒Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State's official acceptance of the implemented solution.
N: No details of the "AI-powered chatbot"
N: No details of the "trusted third-party provider to offer toll-free telephone support to Maine residents."

b. ☒Terms and duration of the support and maintenance will be specified in the contract.
P: Adequate response

c. ☒All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
N: Did NOT respond to this item

d. ☒Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
N: No details of the phone support partner

e. ☒All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
N: Weak response. Covers Okta, but NOT ID.me.

f. ☒All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
N: Weak response. Covers Okta, but NOT ID.me.

g. ☒User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
N: Weak response. Covers Okta, but NOT ID.me.

4. Security

The proposed solutions must provide a robust security system that aligns with the States Security Policies, standards, and Processes, Including:

Comply with or have the following security certifications:

i. ☒National Institute of Standards and Technology (NIST) 800-53
ii. ☒FedRamp
iii. ☒Health Insurance Portability and Accountability Act (HIPAA)
iv. ☒SOC 2 Type II
v. ☒Comply to the following security controls:
vi. ☒DDOS Protections [WN1]
vii. ☒Open Web Application Security Project (OWASP) Top 10
viii. ☒Cross Site Scripting
ix. ☒Structured Query Language (SQL) Injection
x. ☒Authentication bypass
xi. ☒Poorly authenticated APIs
xii. ☒Role based access controls
xiii. ☒Proper session control
xiv. ☒Real-time visibility
xv. ☒Anomalous behavior
xvi. ☒User sign with geo-location tracking
xvii. ☒Geo-blocking capabilities.
xviii. ☒Web Application Firewall [WN1]
xix. ☒System security must include the following security components:
xx. ☒Account take over protections
xxi. ☒Account sign-in Protections
xxii. ☒Behavior detection and evaluation
xxiii. ☒Adaptive AI Technology
xxiv. ☒Bot Protection; identity visitor behavior through analysis, technical and behavioral data.
xxv. ☒The proposed solution must be able to integrate with the State Security Information and Event Monitoring (SIEM) Splunk. Ability to log security information and events.

N: Weak response. Covers Okta, but NOT ID.me.

5. Licensing

☒The State is aware that multiple licensing options are available and will be required to support the proposed solution in its entirety. The State seeks bids which will provide the most cost-effective licensing approach. Bidders are required to provide a detail breakdown for the proposed licensing.

N: Missing "Appendix I section II Licensing"

1. **Training and OCM (Organizational Change Management)**
   a. ☒Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
   b. ☒Training must include technical and administrator training, initial and ongoing as users are added.
   c. ☒Continuous process to ensure Constituents that may have run into issues setting up accounts have help 24/7.
   d. ☒Bidders shall guide the State in OCM engagement for the duration of project planning, transition, and final implementation phase including:
      i. Designing and managing team structures with roles and responsibilities to facilitate automated program delivery, while noting any risks anticipated from the lack of readiness in the organization and staffing.
      ii. Ensure a successful transition for the integration of new processes and technology with stakeholders.
      iii. Organizational readiness assessment

   P: Adequate response

3. **Disaster Recovery**
   a. ☒Availability of ninety-nine-point nine percent (99.9%) of uptime
   b. ☒Capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six (6) hours (i.e., maximum data loss cannot exceed six (6) hours)
   c. ☒Recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours.

   N: Weak response. Covers Okta, but NOT ID.me.

4. **Feature Enhancements**

a. ☒The State is seeking two hundred and fifty (250) hours of time and material for each proposed technology (CIAM), Personalized Dashboard, Disclosure and Consent Management, Data Management, and Recommendation Technology) to allow for specifications and enhancements during the contract period.

P: Strong response

5. **Project Management**

a. ☒The State plans to have its own project manager however, the awarded Bidder must have a project manager that has the primary responsibility for executing the project management tasks associated with the project. The awarded Bidder will:
   i. Work in collaboration with the State's Project Manager
   ii. Align with State Project Management processes and practices.
b. ☒Manage the implementation, executing all activities, tasks, deliverables and resource needs, both state and awarded Bidder.
c. ☒Track project status including managing and tracking all project risks, issues and decisions.
d. ☒Track and report status of deliverables and project status
e. ☒The awarded Bidder will provide their approach for project management and administration services including:
   i. Project Management Methodology
   ii. Project Governance
   iii. Resource Allocation and Schedule Management approach
   iv. Communication Management Approach including status reporting and document repository management.
   v. Risk and Issue Management Methodology
   vi. Change Management Methodology
   vii. Quality Management Methodology

   N: Overall, weak response. Not enough details.

D. Value Added Options (Other)

☒Bidders shall provide value added optional services to address relevant matters that have not been anticipated in this RFP but contribute to successful implementation of the proposed solutions, as well as any technology or services that will reduce risk to the project's quality and continuity. The value-added technology and services will not be included in the evaluation process but may be added during the contract negotiations.

N: None provided

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Active Cyber
DATE: 5/21/2024
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

Section I – Preliminary Information (No points – Eligibility Requirements)

(File #1 App. A, B, C)
☒Done – Pass/Fail by Procurement & RFP Coordinator

Section II Organization Qualifications and Experience

(File #2 – App. D, E + other areas that have no Appendix number but are part of File #2)

1. Overview of the Organization (App. D)

☒Bidders must include three examples of projects which demonstrate their experience and expertise in performing these services as well as highlighting the Bidder's stated qualifications and skills.

Statement of qualifications

☒Client name, contact person, Ph#, email.

Contract history with the state may be considered in rating proposals even if not provided by the bidder.

P, N, Q, or I & Notes: Negative, did not provide telephone or email for any of them. Also had vague/limited description of project and nearly using the same vague language for all three examples. See comment in 2. below

2. Subcontractors (App. E)

☒If subcontractors are to be used, Bidders must provide the name, address, phone number, contact person, and a brief description of the subcontractors' organizational capacity and qualifications.

Business name, contact person, address, ph#, email.

P, N, Q, or I & Notes: Q – on page 6 – they indicate they are "partnering" with Okta ID for identity proofing and Carahsoft as . . . . the sentence can't be seen. But this is in App.D, not E.

3. Organizational Chart (No Appendix)

☒Bidders must provide an organizational chart. The organizational chart must include the project being proposed. Each position must be identified by position title and corresponding to the personnel job descriptions.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Active Cyber
DATE: 5/21/2024
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

P, N, Q, or I & Notes: Negative. Did not include an organizational chart.

4. **Litigation (No App.)**
   ☒Bidders must attach a list of all current litigation in which the Bidder is named and a list of all closed cases that have closed within the past five (5) years in which the Bidder paid the claimant either as part of a settlement or by decree. For each, list the entity bringing suit, the complaint, the accusation, amount, and outcome.
   P, N, Q, or I & Notes: Negative. Bidder did not disclose any response.

5. **Financial Viability (No App.)**
   ☒Bidders must provide a current copy of their Dun & Bradstreet Business Information Report Snapshot.
   P, N, Q, or I - Notes: Negative – Bidder did not provide.

6. **Licensure/Certification (No App.)**
   ☒Bidders *may* provide documentation of any applicable licensure/certification or specific credentials that are related to providing the proposed services of the RFP.
   P, N, Q, or I & Notes: Interesting – Bidder did not provide.

7. **Certificate of Insurance (No App.)**
   ☒Bidders must provide a certificate of insurance on a standard ACORD form (or the equivalent) evidencing the Bidder's general liability, professional liability and any other relevant liability insurance policies that might be associated with the proposed services.
   P, N, Q, or I & Notes: N – Bidder did not provide.

Section III - Proposed Services

(File #3 – App. F, G, H)

1. **Technical Assessment (App. F)**
   ☒Done

2. **Services to be Provided (App. G)**

Note: on App. G Detailed Technical and Functional Requirements Excel spreadsheet, a tab is labeled User Stories. No response is required for Tab 3; these were provided to bidders for clarity and understanding of the expected journey a Constituent will experience.

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Active Cyber
DATE: 5/21/2024
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes: P – link addresses adaptability. Thorough answers.	**1. System security components System security must include the following security components:**
	1) Account Take Over Protections
	a) Account Sign-in Protections
	a) Account Sign-in Protections
	a) Adaptive AI Technology
	b) Bot Protection: identify visitor behavior through analysis of technical and behavioral data.
☒ P, Q, N or I Notes: P – There is an add-on cost.	**2. Identity Proofing must have the ability to provide levels of proofing which will be directly tied to the constituent's level of access.**
	1) Define various levels of id proofing
	2) Document Image Capture
	3) Close coupling with authentication
☒ P, Q, N or I Notes: P – I think it addresses credential theft as it states "shared credentials" as being protected as well	**3. Multi-factor authentication The system must support multi-factor authentication to protect against user impersonation and credential theft.**
☒ P, Q, N or I	**4. Risk-based factors The system must support risk-based factors and scores that are based on factors such as, but not limited to, device and location.**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Active Cyber
DATE: 5/21/2024
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

Notes: P – addresses all factors.	
☒ P, Q, N or I Notes: P – Okta and ID.me address all.	**5. Identity lifecycle management components The system must include the following identity lifecycle management components for risk-based critical applications not limited to end users but also for generic accounts and system/service accounts:**
	1) Identity Creation
	2) Identity provisioning
	3) Attribute maps
	4) Authentication (e.g., password policies and synchronization)

☒ P, Q, N or I Notes: P – addresses all	**6. Security event logging The system must log security information and events.**
	Security Information and Event Management (SIEM) – Splunk
	Cloud Services: Azure, AWS, Oracle, Google
☒ P, Q, N or I Notes: P	**7. Security Certifications The system must comply too or have the following security certifications:**
	1) NIST 800-53
	2) FedRamp
	3) HIPAA
	4) SOC 2 Type II
	Note:

	IRS require a 45-day letter approval for new cloud solutions.
☒ P, Q, N or I Notes: P	**8. SIEM (Splunk) integration The system must be able to integrate with the State of Maine Security Information and Event Monitoring (SIEM) Splunk for Security Operations Center operations.**
☒ P, Q, N or I Notes: P	**9. Core constituent data. The system must maintain a central repository of basic (core) constituent data, that can be used by any SoM application to reduce data redundancy and outdated or inaccurate information while maintaining confidentiality.**
☒ P, Q, N or I Notes: I – addresses processing, integration but does not say specifically they will apply SoM Data Mgmt. Policies. PARTIAL NOT Y OR N OR ON	**11. Data Management. The system must apply the Data Management Rules to the constituent profile data as per the SoM Data Management Policies.**
☒ P, Q, N or I Notes: P	**12. SOM Employee. The system must support multiple identities for SOM employees that work with the portal in a support role.**
	1) SOM Employee identity and credentials for supporting the application.
	2) Constituent identity and credentials to use the state services offered through the portal.

☒ P, Q, N or I	**13. APIs. The system must be able to connect to at least one agency application.**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Active Cyber
DATE: 5/21/2024
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

Notes: P	
	Considerations:
	a) OpenID, OAuth, WS-Fed, SAML, LDAP, Active Directory, Application Programming Interfaces (APIs), Software Development
	b) Develop once and reuse often with other agencies would be ideal
☒ P, Q, N or I Notes: P	**14. User identification matching. The system must be able to match the identity of the portal user to the identity of the same user in the agency system.**
☒ P, Q, N or I Notes: P	**15. Single sign-on. The system must support single sign-on to the agency application.**
☒ P, Q, N or I Notes: I – Does not mention SoM offboarding in timely manner or fraud.	**16. Import user profile data from agency systems. The system must be able to import user data from different SoM applications to ensure offboarding happens in a timely manner, so that government resources are protected from fraud. (example: death records)**
☒ P, Q, N or I Notes: P	**17. History logging.** 1) The system must log all actions taken by:
	a) Constituents
	b) MaineIT support
	Including but not limited to:
	c) who made the change
	d) when the change was made
	e) what changed
☒ P, Q, N or I Notes: N – States it can	**18. Reporting. The logging data (history) must be available for constituent and system dashboards and reporting in general.**

be done through 3rd party systems.	
☒ P, Q, N or I Notes: P	**19. Security Controls. The system must comply to the following security controls:**
	1) DDOS Protections[WN1] ,
	2) OWASP Top 10
	a) Cross Site Scripting,
	b) SQL Injection,
	3) Authentication bypass,
	a) poorly authenticated APIs,
	b) Role based access controls,
	c) proper session control
	4) Real-time visibility,
	5) Anomalous behavior,
	6) User sign with geo-location tracking,
	Geo-blocking capabilities.
	Security controls must include Web Application Firewall [WN1]
☒ P, Q, N or I Notes:	**20. General System Requirements.** 1) Mobile Support with Native App; (iOS and Android)
N – links provided by vendor did not open to any stats. And they did not address 24/7, 4x1 specifically	2) System availability: 24/7 with 4x1-hour outages per year
Did not speak to "cloud infrastructure"	3) Identity relationships must be tracked in the cloud infrastructure.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Active Cyber
DATE: 5/21/2024
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

P - on this one	4) Support responsive web and web browsers.
	a. Supports Windows, Chrome, and Macintosh operating systems
☒ P, Q, N or I Notes: P	**21. Training and Support.** 1) Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
	2) MaineIT will require technical/administrator training. There will be initial training and on-going training as users are added.
	3) Have a continuous process to ensure constituents that may have run into issues setting up accounts can have help 24/7.
☒ P, Q, N or I Notes: Y	**22. Support Requirements** 1) The Bidder will provide support, and maintenance for the solution to begin immediately after receiving the State's official acceptance of the implemented solution.
	2) Support and maintenance will be provided for the terms and duration specified in the contract.
	3) The Bidder will address all questions and reported problems related to the technical and functional operation of the system.
	4) The Bidder must provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours: 8:00 a.m. to 5:00 p.m. Eastern Standard Time.
	5) As part of the maintenance agreement, the Bidder will make all product releases and upgrades available to the State at no additional charge.
	6) All release and upgrades shall be implemented and tested by the Bidder, outside of the normal operating hours of the State government.
	7) User testing shall occur during normal State business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State government.
☒ P, Q, N or I	**23. Hosting** Solution can comply with MaineIT remote hosting policies. a) Remote Hosting Policy http://maine.gov/oit/policies/RemoteHostingPolicy.pdf

Notes: N – vendor did not specifically address SoM policy adherence.	b) Hosting Customization Policy http://maine.gov/oit/policies/HostingCustomizationPolicy.pdf
☒ P, Q, N or I Notes: N – two items not addressed adequately.	**24. Disaster Recovery** Proposed Solution can comply with MaineIT security requirements and remote hosting requirements, without requiring waivers, before contract finalization.
Did address	1) Maintaining an availability metric of ninety-nine-point nine percent (99.9%) of uptime
Vendor has stated 24hr for Recovery Time. With 1 hour read only mode.	2) Ensuring the capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six hours (i.e., maximum data loss cannot exceed six (6) hours);
Did address.	3) Ensuring a recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours;
Response time not addressed to SoM needs.	4) Ensuring the hosting environment provides adequate capacity to ensure that, under ethernet connectivity to the client device, data inquiry/lookup response is within three (3) seconds, and data modification response is within five (5) seconds;
Did not say they could comply.	5) Providing the Department at least thirty (30) calendar day advance written notice of any material change in network operations or architecture;
Did not say they could comply, same answer as above.	6) Ensuring any planned material change in network operations or architecture cannot be made without the prior written consent of the Department; and Outlining of all Service Level Agreements (SLAs) for technical support (the awarded Bidder shall be open to negotiation to ensure the SLAs meet the Department’s needs

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Active Cyber
DATE: 5/21/2024
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

☒1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
P, N, Q, or I & Notes: N – one paragraph of description is not a full description of a solution this complicated.

☒1b) Detailed description of the technologies, software and / or hardware for each of the components.
P, N, Q, or I & Notes: N – sparce description is not a full description of a solution this complicated.

☒1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.
P, N, Q, or I & Notes: N – three bullets of description is not a full description of a solution this complicated.

☒1d) Description of the overall platform and architecture of the proposed solution(s).
P, N, Q, or I & Notes: N - N – one paragraph & one simplistic graphic is not a full description of a solution this complicated.

☒1e) Description of any third-party software or partnerships required for the proposed Solution(s).
P, N, Q, or I & Notes: N – sparce description is not a full description of a solution this complicated.

☒2a) A detailed timeline and description of milestones, deliverables, tasks
P, N, Q, or I & Notes: N – not detailed adequately, although timeline was good.

☒2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through

Implementation Period and Post Implementation – Support period
P, N, Q, or I & Notes: N – resumes not supplied – description of plan as one bullet item under each is not adequate.

☒2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
P, N, Q, or I & Notes: N – missing detailed deliverables, deliverables are generically listed.

☒2d) Average time to market for each component.
P, N, Q, or I & Notes: N – marketing language of Okta product provided with no time to marked outlined.

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. ☒Capture Constituent Identity and profile data.
   P, N, Q, or I & Notes:
b. ☒Provide identity provisioning and deprovisioning.
   P, N, Q, or I & Notes:
c. ☒Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
   i. Identity Creation
   ii. Identity provisioning
   iii. Attribute maps
   iv. Authentication (e.g., password policies and synchronization)
      P, N, Q, or I & Notes: P
d. ☒Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies.
   P, N, Q, or I & Notes: N – boiler plate marketing language, did not speak to SoM methods or agencies.

e. ☒Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
P, N, Q, or I & Notes: N – boiler plate marketing language, did not speak to SoM methods or agencies.

f. ☒Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.
P, N, Q, or I & Notes: N – states that Okta extensibility enables but does not describe.

g. ☒Allow for multiple role selections for the following identities:
   i. Individual
   ii. Business Owner
   iii. Support multiple identities for State employees that work with the portal in a support role:
      (a) SOM Employee identity and credentials for supporting the application.
      (b) Constituent identity and credentials to use the state services offered through the portal.
   iv. Multi role individual (Individual and Business Owner)
   P, N, Q, or I & Notes: P

h. ☒Have the ability to provide levels of proofing which will be directly tied to the Constituent's level of consent given.
P, N, Q, or I & Notes: P

i. ☒Support multi-factor authentication to protect against user impersonation and credential theft.
P, N, Q, or I & Notes: P

B.2. ☐The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.
P, N, Q, or I & Notes: N – Bidder referenced being "inspired" by ILogin once logged in, saw 4 apps but was not very polished.

a. Disclosure and Consent Management

The desire of the State is to be as transparent as possible and respect the privacy of the individual interacting with the Constituents' Portal. Consent is a core tenant of maintaining the public trust in the Constituents' Portal and will be a foundational component of the architecture.

The Disclosure and Consent Management solution shall include:

i. ☒Granular consent management that encompasses the automated functions necessary to create, modify, revoke, and manage Constituent consents. Implementation and User support area will done.
ii. ☒Allow users the ability to opt-in and opt-out of data sharing and services within the Constituents' portal.
iii. ☒Obtain user consent both in an interactive and set preference mode for a variety of transactions on the Portal.
iv. ☒Support administrative users' management of standard legal disclaimers and data classification for transactions.
v. ☒Highly configurable with version control and history tracking for consent language.
vi. ☒Ability for end user to access a retrievable log of granted consent and data usage on the portal derived from the consent.

P, N, Q, or I & Notes: P This section was well done.

b. Recommendation Technology

The State is seeking options which, while maintaining individual privacy, will collect and analyze data about user interactions, behavior, and preferences. The expected outcome of this will be to provide insights and intelligence that help the State make informed decisions and improve Constituent experiences.

i. ☒From the user perspective, the portal should be able to make real-time recommendations for related services. "Develop a recommendation engine" but unsure if they have something to offer or they will create it. The answers were very generic and did not provide much detail.
ii. ☒Data captured in this environment must be obfuscated, as to not allow any party to directly target or track the preferences of an individual or their usage of the portal.
iii. ☒Solution providers should discuss in detail their use, storage, destruction of metadata, and tracking technologies with emphasis on how their offering provides analytical insights while protecting the individual user privacy.

P, N, Q, or I & Notes: P – overall well written.

c. Data Management

The State is seeking the ability for the portal's Constituent identity to be linked to records maintained by individual State agencies. The proposed solution will include:

- i. ☒Capabilities to streamline the sharing of data between State systems, including
  - i. The identity assurance level
  - ii. Agency to user notifications
  - iii. Verification of user consent
  - iv. Identity resolution
  - v. Data sharing between agencies.
- ii. ☒Maintain a central repository of basic (core) Constituent data, that can be used by any State application to reduce data redundancy, and outdated or inaccurate information while maintaining confidentiality.
- iii. ☒Ability to integrate with State applications using, OpenID, OAuth, Web Services Federation Protocol (WS-Fed), Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), Active Directory, Application Programming Interface (API) or equivalent protocols.
- iv. ☒Ability to match the identity of the portal user to the identity of the same user in the Agency system.
- v. ☒Log all actions taken by:
  - i. Constituents
  - ii. MaineIT Support, including:
    - (a) Who made the change
    - (b) When the change was made
    - (c) What changed to and from
- vi. ☒Logging data must be available for system dashboards and reporting.

P, N, Q, or I & Notes: P – overall well done.

d. Customer Service

The State is seeking solution(s) to provide 24/7/365 customer service to Constituents regardless of their location or technical abilities.

- i. ☒Support Constituents with personalized and timely assistance.
- ii. ☒Provide the state options to support our Constituents across multiple channels including, but not limited to phone, email, chat, etc.

P, N, Q, or I & Notes: P – Multi-channel, phone included.

C.1. General System

a. ☒Mobile support with native app (iOS and Android)
b. ☒System availability: 24/7 with a maximum of four (4) 1-hour outages per year
c. ☒Identity relationships must be tracked in the cloud infrastructure.
d. ☒Support responsive web and web browsers.
    i. ☒Supports Windows, Chrome, and Macintosh operating systems.

P, N, Q, or I & Notes: P

C.2. ☐Compliance with MaineIT Policies & Standards

a. Architecture Compliance Policy
b. System and Services Acquisition Policy and Procedures (SA-1)
c. Application Deployment Certification Policy
d. Digital Accessibility Policy
e. Remote Hosting Policy
f. Data Exchange Policy
g. Information Security Policy
h. Access Control Policy (AC-1)
i. Access Control Procedures for Users (AC-2)
j. Risk Assessment Policy and Procedures (RA-1)
k. Vulnerability Scanning Procedure (RA-5)
l. Security Assessment and Authorization Policy and Procedures (CA-1)
m. System and Information Integrity Policy and Procedures (SI-1)
n. Configuration Management Policy (CM-1)
o. Web Standards

P, N, Q, or I & Notes: N- they provide Okta's and ID.me certs but do not say specifically they will adhere to SoM.

C.3. Support and Maintenance

a. ☒Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State's official acceptance of the implemented solution.
   P, N, Q, or I & Notes: P

b. ☒Terms and duration of the support and maintenance will be specified in the contract.
P, N, Q, or I & Notes: P

c. ☒All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
P, N, Q, or I & Notes: P

d. ☒Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
P, N, Q, or I & Notes: P

e. ☒All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
P, N, Q, or I & Notes: P

f. ☒All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
P, N, Q, or I & Notes: P

g. ☒User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
P, N, Q, or I & Notes: P

4. Security

The proposed solutions must provide a robust security system that aligns with the States Security Policies, standards, and Processes, Including:

Comply with or have the following security certifications:

i. ☐National Institute of Standards and Technology (NIST) 800-53
ii. ☐FedRamp
iii. ☐Health Insurance Portability and Accountability Act (HIPAA)
iv. ☐SOC 2 Type II
v. ☐Comply to the following security controls:
vi. ☐DDOS Protections [WN1]
vii. ☐Open Web Application Security Project (OWASP) Top 10
viii. ☐Cross Site Scripting
ix. ☐Structured Query Language (SQL) Injection
x. ☐Authentication bypass

xi. ☐Poorly authenticated APIs
xii. ☐Role based access controls
xiii. ☐Proper session control
xiv. ☐Real-time visibility
xv. ☐Anomalous behavior
xvi. ☐User sign with geo-location tracking
xvii. ☐Geo-blocking capabilities.
xviii. ☐Web Application Firewall [WN1]
xix. ☐System security must include the following security components:
xx. ☐Account take over protections
xxi. ☐Account sign-in Protections
xxii. ☐Behavior detection and evaluation
xxiii. ☐Adaptive AI Technology
xxiv. ☐Bot Protection; identity visitor behavior through analysis, technical and behavioral data.
xxv. ☐The proposed solution must be able to integrate with the State Security Information and Event Monitoring (SIEM) Splunk. Ability to log security information and events.

P, N, Q, or I & Notes: P all areas

5. Licensing

☒The State is aware that multiple licensing options are available and will be required to support the proposed solution in its entirety. The State seeks bids which will provide the most cost-effective licensing approach. Bidders are required to provide a detail breakdown for the proposed licensing.

P, N, Q, or I & Notes: N – Bidder referenced App. I but there was no App. I attached.

1. Training and OCM (Organizational Change Management)

a. ☒Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
b. ☒Training must include technical and administrator training, initial and ongoing as users are added.
c. ☒Continuous process to ensure Constituents that may have run into issues

setting up accounts have help 24/7.

d. ☒Bidders shall guide the State in OCM engagement for the duration of project planning, transition, and final implementation phase including:
   i. Designing and managing team structures with roles and responsibilities to facilitate automated program delivery, while noting any risks anticipated from the lack of readiness in the organization and staffing.
   ii. Ensure a successful transition for the integration of new processes and technology with stakeholders.
   iii. Organizational readiness assessment

P, N, Q, or I & Notes: N – but could not find the Security, identity and access management training piece.

3. Disaster Recovery

a. ☒Availability of ninety-nine-point nine percent (99.9%) of uptime
b. ☒Capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six (6) hours (i.e., maximum data loss cannot exceed six (6) hours)
c. ☒Recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours.

P, N, Q, or I & Notes: P

4. Feature Enhancements

a. ☒The State is seeking two hundred and fifty (250) hours of time and material for each proposed technology (CIAM), Personalized Dashboard, Disclosure and Consent Management, Data Management, and Recommendation Technology) to allow for specifications and enhancements during the contract period.

P, N, Q, or I & Notes:P – Did they actually offer us more than we asked for?

5. Project Management

a. ☒The State plans to have its own project manager however, the awarded Bidder must have a project manager that has the primary responsibility for executing the project management tasks associated with the project. The awarded Bidder will:
   i. Work in collaboration with the State's Project Manager
   ii. Align with State Project Management processes and practices.

b. ☒Manage the implementation, executing all activities, tasks, deliverables and resource needs, both state and awarded Bidder.
c. ☒Track project status including managing and tracking all project risks, issues and decisions.
d. ☒Track and report status of deliverables and project status
e. ☒The awarded Bidder will provide their approach for project management and administration services including:
    i. Project Management Methodology
    ii. Project Governance
    iii. Resource Allocation and Schedule Management approach
    iv. Communication Management Approach including status reporting and document repository management.
    v. Risk and Issue Management Methodology
    vi. Change Management Methodology
    vii. Quality Management Methodology

    P, N, Q, or I & Notes: N – they wrote back requirements but did not provide specifics.

D. Value Added Options (Other)

☒Bidders shall provide value added optional services to address relevant matters that have not been anticipated in this RFP but contribute to successful implementation of the proposed solutions, as well as any technology or services that will reduce risk to the project's quality and continuity. The value-added technology and services will not be included in the evaluation process but may be added during the contract negotiations.

P, N, Q, or I & Notes: I – nothing provided.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Carasoft
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

Section I – Preliminary Information (No points – Eligibility Requirements)

(File #1 App. A, B, C)
☒Done – Pass/Fail by Procurement & RFP Coordinator

Section II Organization Qualifications and Experience

(File #2 – App. D, E + other areas that have no Appendix number but are part of File #2)

1. Overview of the Organization (App. D)

☒Bidders must include three examples of projects which demonstrate their experience and expertise in performing these services as well as highlighting the Bidder's stated qualifications and skills.

Statement of qualifications

☒Client name, contact person, Ph#, email.

Contract history with the state may be considered in rating proposals even if not provided by the bidder.

P, N, Q, or I & Notes:Q Contact info not provided

2. Subcontractors (App. E)

☒If subcontractors are to be used, Bidders must provide the name, address, phone number, contact person, and a brief description of the subcontractors' organizational capacity and qualifications.

Business name, contact person, address, ph#, email.

P, N, Q, or I & Notes:P

3. Organizational Chart (No Appendix)

☒Bidders must provide an organizational chart. The organizational chart must include the project being proposed. Each position must be identified by position title and corresponding to the personnel job descriptions.

P, N, Q, or I & Notes:P

4. Litigation (No App.)

☒Bidders must attach a list of all current litigation in which the Bidder is named and a list of all closed cases that have closed within the past five (5) years in which the Bidder paid the claimant either as part of a settlement or by decree. For each, list the entity bringing suit, the complaint, the accusation, amount, and outcome.
P, N, Q, or I & Notes:P

5. **Financial Viability (No App.)**
☒Bidders must provide a current copy of their Dun & Bradstreet Business Information Report Snapshot.
P, N, Q, or I - Notes:P

6. **Licensure/Certification (No App.)**
☒Bidders *may* provide documentation of any applicable licensure/certification or specific credentials that are related to providing the proposed services of the RFP.
P, N, Q, or I & Notes:P

7. **Certificate of Insurance (No App.)**
☒Bidders must provide a certificate of insurance on a standard ACORD form (or the equivalent) evidencing the Bidder's general liability, professional liability and any other relevant liability insurance policies that might be associated with the proposed services.
P, N, Q, or I & Notes:P

Section III - Proposed Services

(File #3 – App. F, G, H)

1. **Technical Assessment (App. F)**
☒Done

2. **Services to be Provided (App. G)**

Note: on App. G Detailed Technical and Functional Requirements Excel spreadsheet, a tab is labeled User Stories. No response is required for Tab 3; these were provided to bidders for clarity and understanding of the expected journey a Constituent will experience.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Carasoft
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes:P	**1. System security components System security must include the following security components:**
	1) Account Take Over Protections
	a) Account Sign-in Protections
	a) Account Sign-in Protections
	a) Adaptive AI Technology
	b) Bot Protection: identify visitor behavior through analysis of technical and behavioral data.
☒ P, Q, N or I Notes: P	**2. Identity Proofing must have the ability to provide levels of proofing which will be directly tied to the constituent's level of access.**
	1) Define various levels of id proofing
	2) Document Image Capture
	3) Close coupling with authentication
☒ P, Q, N or I Notes: P	**3. Multi-factor authentication The system must support multi-factor authentication to protect against user impersonation and credential theft.**
☒ P, Q, N or I Notes: P	**4. Risk-based factors The system must support risk-based factors and scores that are based on factors such as, but not limited to, device and location.**
☒ P, Q, N or I Notes: P	**5. Identity lifecycle management components The system must include the following identity lifecycle management components for risk-based critical applications not limited to end users but also for generic accounts and system/service accounts:**
P	1) Identity Creation
P	2) Identity provisioning
P	3) Attribute maps
P	4) Authentication (e.g., password policies and synchronization)

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Carasoft
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes:P	**6. Security event logging The system must log security information and events.**
	Security Information and Event Management (SIEM) – Splunk
	Cloud Services: Azure, AWS, Oracle, Google
☒ P, Q, N or I Notes:N	**7. Security Certifications The system must comply too or have the following security certifications:**
Partial	1) NIST 800-53
N	2) FedRamp
comply	3) HIPAA
comply	4) SOC 2 Type II
	Note:
	IRS require a 45-day letter approval for new cloud solutions.
☒ P, Q, N or I Notes:P	**8. SIEM (Splunk) integration The system must be able to integrate with the State of Maine Security Information and Event Monitoring (SIEM) Splunk for Security Operations Center operations.**
☒ P, Q, N or I Notes:P	**9. Core constituent data. The system must maintain a central repository of basic (core) constituent data, that can be used by any SoM application to reduce data redundancy and outdated or inaccurate information while maintaining confidentiality.**
☒ P, Q, N or I Notes:P	**11. Data Management. The system must apply the Data Management Rules to the constituent profile data as per the SoM Data Management Policies.**
☒ P, Q, N or I Notes:P	**12. SOM Employee. The system must support multiple identities for SOM employees that work with the portal in a support role.**
P	1) SOM Employee identity and credentials for supporting the application.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Carasoft
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

P	2) Constituent identity and credentials to use the state services offered through the portal.

☒ P, Q, N or I Notes:P	**13. APIs. The system must be able to connect to at least one agency application.**
	Considerations:
	a) OpenID, OAuth, WS-Fed, SAML, LDAP, Active Directory, Application Programming Interfaces (APIs), Software Development
	b) Develop once and reuse often with other agencies would be ideal
☒ P, Q, N or I Notes:P	**14. User identification matching. The system must be able to match the identity of the portal user to the identity of the same user in the agency system.**
☒ P, Q, N or I Notes:P	**15. Single sign-on. The system must support single sign-on to the agency application.**
☒ P, Q, N or I Notes:P	**16. Import user profile data from agency systems. The system must be able to import user data from different SoM applications to ensure offboarding happens in a timely manner, so that government resources are protected from fraud. (example: death records)**
☒ P, Q, N or I Notes:P	**17. History logging.** 1) The system must log all actions taken by:
P	a) Constituents
P	b) MaineIT support
P	Including but not limited to:
P	c) who made the change
P	d) when the change was made
P	e) what changed

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Carasoft
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes:P	**18. Reporting. The logging data (history) must be available for constituent and system dashboards and reporting in general.**
☒ P, Q, N or I Notes:P	**19. Security Controls. The system must comply to the following security controls:**
P	1) DDOS Protections[WN1] ,
P	2) OWASP Top 10
P	a) Cross Site Scripting,
P	b) SQL Injection,
P	3) Authentication bypass,
P	a) poorly authenticated APIs,
P	b) Role based access controls,
P	c) proper session control
P	4) Real-time visibility,
P	5) Anomalous behavior,
P	6) User sign with geo-location tracking,
P	Geo-blocking capabilities.
P	Security controls must include Web Application Firewall [WN1]
☒ P, Q, N or I Notes:P	**20. General System Requirements.** 1) Mobile Support with Native App; (iOS and Android)
P	2) System availability: 24/7 with 4x1-hour outages per year
P	3) Identity relationships must be tracked in the cloud infrastructure.
P	4) Support responsive web and web browsers.
P	a. Supports Windows, Chrome, and Macintosh operating systems
☒ P, Q, N or I Notes:P	**21. Training and Support.** 1) Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Carasoft
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

P	2) MaineIT will require technical/administrator training. There will be initial training and on-going training as users are added.
P	3) Have a continuous process to ensure constituents that may have run into issues setting up accounts can have help 24/7.
☒ P, Q, N or I Notes:P	**22. Support Requirements** 1) The Bidder will provide support, and maintenance for the solution to begin immediately after receiving the State's official acceptance of the implemented solution.
P	2) Support and maintenance will be provided for the terms and duration specified in the contract.
P	3) The Bidder will address all questions and reported problems related to the technical and functional operation of the system.
P	4) The Bidder must provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours: 8:00 a.m. to 5:00 p.m. Eastern Standard Time.
P	5) As part of the maintenance agreement, the Bidder will make all product releases and upgrades available to the State at no additional charge.
P	6) All release and upgrades shall be implemented and tested by the Bidder, outside of the normal operating hours of the State government.
P	7) User testing shall occur during normal State business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State government.
☒ P, Q, N or I Notes:P	**23. Hosting** Solution can comply with MaineIT remote hosting policies. a) Remote Hosting Policy http://maine.gov/oit/policies/RemoteHostingPolicy.pdf b) Hosting Customization Policy http://maine.gov/oit/policies/HostingCustomizationPolicy.pdf
☒ P, Q, N or I Notes:Q on the 30	**24. Disaster Recovery** Proposed Solution can comply with MaineIT security requirements and remote hosting requirements, without requiring waivers, before contract finalization.

day notice	
P	1) Maintaining an availability metric of ninety-nine-point nine percent (99.9%) of uptime
P	2) Ensuring the capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six hours (i.e., maximum data loss cannot exceed six (6) hours);
P	3) Ensuring a recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours;
P	4) Ensuring the hosting environment provides adequate capacity to ensure that, under ethernet connectivity to the client device, data inquiry/lookup response is within three (3) seconds, and data modification response is within five (5) seconds;
Partial	5) Providing the Department at least thirty (30) calendar day advance written notice of any material change in network operations or architecture;
P	6) Ensuring any planned material change in network operations or architecture cannot be made without the prior written consent of the Department; and Outlining of all Service Level Agreements (SLAs) for technical support (the awarded Bidder shall be open to negotiation to ensure the SLAs meet the Department's needs

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

☒1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
P, N, Q, or I & Notes:P

☒1b) Detailed description of the technologies, software and / or hardware for each of the components.
P, N, Q, or I & Notes:P

☒1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Carasoft
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

P, N, Q, or I & Notes:P

☒1d) Description of the overall platform and architecture of the proposed solution(s).
P, N, Q, or I & Notes:P

☒1e) Description of any third-party software or partnerships required for the proposed Solution(s).
P, N, Q, or I & Notes:P

☒2a) A detailed timeline and description of milestones, deliverables, tasks
P, N, Q, or I & Notes:N not detailed

☒2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period
P, N, Q, or I & Notes:N Not provided

☒2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
P, N, Q, or I & Notes:N not provided

☒2d) Average time to market for each component.
P, N, Q, or I & Notes:Q not provided

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State’s, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual’s identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. ☒Capture Constituent Identity and profile data.

P, N, Q, or I & Notes:P

b. ☒Provide identity provisioning and deprovisioning.
P, N, Q, or I & Notes:P

c. ☒Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
  i. Identity Creation
  ii. Identity provisioning
  iii. Attribute maps
  iv. Authentication (e.g., password policies and synchronization)
  P, N, Q, or I & Notes:P

d. ☒Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies.
P, N, Q, or I & Notes:P

e. ☒Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
P, N, Q, or I & Notes:P

f. ☒Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.
P, N, Q, or I & Notes:Q didn’t describe if biometric could be added

g. ☒Allow for multiple role selections for the following identities:
  i. Individual
  ii. Business Owner
  iii. Support multiple identities for State employees that work with the portal in a support role:
    (a) SOM Employee identity and credentials for supporting the application.
    (b) Constituent identity and credentials to use the state services offered through the portal.
  iv. Multi role individual (Individual and Business Owner)
  P, N, Q, or I & Notes:P

h. ☒Have the ability to provide levels of proofing which will be directly tied to the Constituent’s level of consent given.
P, N, Q, or I & Notes:N not answered

i. ☒Support multi-factor authentication to protect against user impersonation and credential theft.
P, N, Q, or I & Notes:P

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Carasoft
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

B.2. ☒The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.
P, N, Q, or I & Notes:P

a. Disclosure and Consent Management

The desire of the State is to be as transparent as possible and respect the privacy of the individual interacting with the Constituents' Portal. Consent is a core tenant of maintaining the public trust in the Constituents' Portal and will be a foundational component of the architecture.

The Disclosure and Consent Management solution shall include:

i. ☒Granular consent management that encompasses the automated functions necessary to create, modify, revoke, and manage Constituent consents.
ii. ☒Allow users the ability to opt-in and opt-out of data sharing and services within the Constituents' portal.
iii. ☒Obtain user consent both in an interactive and set preference mode for a variety of transactions on the Portal.
iv. ☐Support administrative users' management of standard legal disclaimers and data classification for transactions.
v. ☒Highly configurable with version control and history tracking for consent language.
vi. ☒Ability for end user to access a retrievable log of granted consent and data usage on the portal derived from the consent.

P, N, Q, or I & Notes:Q didn't mention legal disclaimers

b. Recommendation Technology

The State is seeking options which, while maintaining individual privacy, will collect and analyze data about user interactions, behavior, and preferences. The

expected outcome of this will be to provide insights and intelligence that help the State make informed decisions and improve Constituent experiences.

i. ☒From the user perspective, the portal should be able to make real-time recommendations for related services.
ii. ☐Data captured in this environment must be obfuscated, as to not allow any party to directly target or track the preferences of an individual or their usage of the portal.
iii. ☐Solution providers should discuss in detail their use, storage, destruction of metadata, and tracking technologies with emphasis on how their offering provides analytical insights while protecting the individual user privacy.

P, N, Q, or I & Notes:Q doesn’t mention data obfuscation or meta destruction

c. Data Management

The State is seeking the ability for the portal’s Constituent identity to be linked to records maintained by individual State agencies. The proposed solution will include:

i. ☒Capabilities to streamline the sharing of data between State systems, including
    i. The identity assurance level
    ii. Agency to user notifications
    iii. Verification of user consent
    iv. Identity resolution
    v. Data sharing between agencies.
ii. ☒Maintain a central repository of basic (core) Constituent data, that can be used by any State application to reduce data redundancy, and outdated or inaccurate information while maintaining confidentiality.
iii. ☒Ability to integrate with State applications using, OpenID, OAuth, Web Services Federation Protocol (WS-Fed), Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), Active Directory, Application Programming Interface (API) or equivalent protocols.
iv. ☒Ability to match the identity of the portal user to the identity of the same user in the Agency system.
v. ☒Log all actions taken by:
    i. Constituents
    ii. MaineIT Support, including:
        (a) Who made the change
        (b) When the change was made

(c) What changed to and from

vi. ☐Logging data must be available for system dashboards and reporting.

P, N, Q, or I & Notes:Q desn't say if logging will be available

d. Customer Service

The State is seeking solution(s) to provide 24/7/365 customer service to Constituents regardless of their location or technical abilities.

i. ☒Support Constituents with personalized and timely assistance.
ii. ☒Provide the state options to support our Constituents across multiple channels including, but not limited to phone, email, chat, etc.

P, N, Q, or I & Notes: P

C.1. General System

a. ☒Mobile support with native app (iOS and Android)
b. ☒System availability: 24/7 with a maximum of four (4) 1-hour outages per year
c. ☒Identity relationships must be tracked in the cloud infrastructure.
d. ☒Support responsive web and web browsers.
    i. ☒Supports Windows, Chrome, and Macintosh operating systems.

P, N, Q, or I & Notes:P

C.2. ☒Compliance with MaineIT Policies & Standards

a. Architecture Compliance Policy
b. System and Services Acquisition Policy and Procedures (SA-1)
c. Application Deployment Certification Policy
d. Digital Accessibility Policy
e. Remote Hosting Policy
f. Data Exchange Policy
g. Information Security Policy
h. Access Control Policy (AC-1)
i. Access Control Procedures for Users (AC-2)
j. Risk Assessment Policy and Procedures (RA-1)
k. Vulnerability Scanning Procedure (RA-5)
l. Security Assessment and Authorization Policy and Procedures (CA-1)

m. System and Information Integrity Policy and Procedures (SI-1)
n. Configuration Management Policy (CM-1)
o. Web Standards

P, N, Q, or I & Notes:P

C.3. Support and Maintenance

a. ☒Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State's official acceptance of the implemented solution.
P, N, Q, or I & Notes:P

b. ☒Terms and duration of the support and maintenance will be specified in the contract.
P, N, Q, or I & Notes:P

c. ☒All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
P, N, Q, or I & Notes:P

d. ☒Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
P, N, Q, or I & Notes:Q doesn't say toll free

e. ☒All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
P, N, Q, or I & Notes:

f. ☒All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
P, N, Q, or I & Notes:Q.Doesn't say bidder will implement

g. ☒User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
P, N, Q, or I & Notes:P

4. Security

The proposed solutions must provide a robust security system that aligns with the States Security Policies, standards, and Processes, Including:

Comply with or have the following security certifications:

i. ☐National Institute of Standards and Technology (NIST) 800-53
ii. ☐FedRamp
iii. ☐Health Insurance Portability and Accountability Act (HIPAA)
iv. ☐SOC 2 Type II
v. ☐Comply to the following security controls:
vi. ☐DDOS Protections [WN1]
vii. ☐Open Web Application Security Project (OWASP) Top 10
viii. ☐Cross Site Scripting
ix. ☐Structured Query Language (SQL) Injection
x. ☐Authentication bypass
xi. ☐Poorly authenticated APIs
xii. ☐Role based access controls
xiii. ☐Proper session control
xiv. ☐Real-time visibility
xv. ☐Anomalous behavior
xvi. ☐User sign with geo-location tracking
xvii. ☐Geo-blocking capabilities.
xviii. ☐Web Application Firewall [WN1]
xix. ☐System security must include the following security components:
xx. ☐Account take over protections
xxi. ☐Account sign-in Protections
xxii. ☐Behavior detection and evaluation
xxiii. ☐Adaptive AI Technology
xxiv. ☐Bot Protection; identity visitor behavior through analysis, technical and behavioral data.
xxv. ☐The proposed solution must be able to integrate with the State Security Information and Event Monitoring (SIEM) Splunk. Ability to log security information and events.

P, N, Q, or I & Notes: N appendix G didn't cover these

5. Licensing

☒The State is aware that multiple licensing options are available and will be required to support the proposed solution in its entirety. The State seeks bids

which will provide the most cost-effective licensing approach. Bidders are required to provide a detail breakdown for the proposed licensing.
P, N, Q, or I & Notes:Q don’t have Appendix I

1. **Training and OCM (Organizational Change Management)**
   a. ☒Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
   b. ☒Training must include technical and administrator training, initial and ongoing as users are added.
   c. ☒Continuous process to ensure Constituents that may have run into issues setting up accounts have help 24/7.
   d. ☒Bidders shall guide the State in OCM engagement for the duration of project planning, transition, and final implementation phase including:
      i. Designing and managing team structures with roles and responsibilities to facilitate automated program delivery, while noting any risks anticipated from the lack of readiness in the organization and staffing.
      ii. Ensure a successful transition for the integration of new processes and technology with stakeholders.
      iii. Organizational readiness assessment

P, N, Q, or I & Notes:P

3. **Disaster Recovery**
   a. ☒Availability of ninety-nine-point nine percent (99.9%) of uptime
   b. ☒Capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six (6) hours (i.e., maximum data loss cannot exceed six (6) hours)
   c. ☒Recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours.

P, N, Q, or I & Notes:Q only covered Ping

4. **Feature Enhancements**

a. ☒The State is seeking two hundred and fifty (250) hours of time and material for each proposed technology (CIAM), Personalized Dashboard, Disclosure and

Consent Management, Data Management, and Recommendation Technology) to allow for specifications and enhancements during the contract period.

P, N, Q, or I & Notes:P

5. Project Management

a. ☒The State plans to have its own project manager however, the awarded Bidder must have a project manager that has the primary responsibility for executing the project management tasks associated with the project. The awarded Bidder will:
   i. Work in collaboration with the State's Project Manager
   ii. Align with State Project Management processes and practices.
b. ☒Manage the implementation, executing all activities, tasks, deliverables and resource needs, both state and awarded Bidder.
c. ☒Track project status including managing and tracking all project risks, issues and decisions.
d. ☒Track and report status of deliverables and project status
e. ☒The awarded Bidder will provide their approach for project management and administration services including:
   i. Project Management Methodology
   ii. Project Governance
   iii. Resource Allocation and Schedule Management approach
   iv. Communication Management Approach including status reporting and document repository management.
   v. Risk and Issue Management Methodology
   vi. Change Management Methodology
   vii. Quality Management Methodology

P, N, Q, or I & Notes:P

D. Value Added Options (Other)

☒Bidders shall provide value added optional services to address relevant matters that have not been anticipated in this RFP but contribute to successful implementation of the proposed solutions, as well as any technology or services that will reduce risk to the project's quality and continuity. The value-added technology and services will not be included in the evaluation process but may be added during the contract negotiations.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Carasoft
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

P, N, Q, or I & Notes:P

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: CarahSoft
DATE: 06032024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

Section I – Preliminary Information (No points – Eligibility Requirements)

(File #1 App. A, B, C)
☒Done – Pass/Fail by Procurement & RFP Coordinator

Section II Organization Qualifications and Experience

(File #2 – App. D, E + other areas that have no Appendix number but are part of File #2)

1. **Overview of the Organization (App. D)**
☒Bidders must include three examples of projects which demonstrate their experience and expertise in performing these services as well as highlighting the Bidder's stated qualifications and skills.

Statement of qualifications
☒Client name, contact person, Ph#, email.
Contract history with the state may be considered in rating proposals even if not provided by the bidder.

P, **N**, Q, or I & Notes:
In their reference examples, Publicis Sapient has no experience

2. **Subcontractors (App. E)**
☒If subcontractors are to be used, Bidders must provide the name, address, phone number, contact person, and a brief description of the subcontractors' organizational capacity and qualifications.
Business name, contact person, address, ph#, email.
P, **N**, Q, or I & Notes:
Subcontractor contact information not included

3. **Organizational Chart (No Appendix)**
☒Bidders must provide an organizational chart. The organizational chart must include the project being proposed. Each position must be identified by position title and corresponding to the personnel job descriptions.
P, **N**, Q, or I & Notes:
Does not include details or subcontractor roles

4. **Litigation (No App.)**

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: CarahSoft
DATE: 06032024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

☒Bidders must attach a list of all current litigation in which the Bidder is named and a list of all closed cases that have closed within the past five (5) years in which the Bidder paid the claimant either as part of a settlement or by decree. For each, list the entity bringing suit, the complaint, the accusation, amount, and outcome.

P, N, Q, or I & Notes:

No attachments

5. **Financial Viability (No App.)**

☒Bidders must provide a current copy of their Dun & Bradstreet Business Information Report Snapshot.

P, N, Q, or **I** - Notes:

Historically revenue reported for Carahsoft, no Dun and Bradstreet report, only their DB number

Nothing of note for subcontractors

6. **Licensure/Certification (No App.)**

☒Bidders *may* provide documentation of any applicable licensure/certification or specific credentials that are related to providing the proposed services of the RFP.

P, N, Q, or **I** & Notes:

Provided additional information around adobe experience cloud security

7. **Certificate of Insurance (No App.)**

☒Bidders must provide a certificate of insurance on a standard ACORD form (or the equivalent) evidencing the Bidder's general liability, professional liability and any other relevant liability insurance policies that might be associated with the proposed services.

P, N, Q, or I & Notes:

Section III - Proposed Services

(File #3 – App. F, G, H)

1. **Technical Assessment (App. F)**

☒Done

2. **Services to be Provided (App. G)**

Note: on App. G Detailed Technical and Functional Requirements Excel spreadsheet, a tab is labeled User Stories. No response is required for Tab 3; these were provided to bidders for clarity and understanding of the expected journey a Constituent will experience.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: CarahSoft
DATE: 06032024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, **N** or I Notes: No explanation given, which technology or subcontractor provides service	1. **System security components System security must include the following security components:**
	1) Account Take Over Protections
	a) Account Sign-in Protections
	a) Account Sign-in Protections
	a) Adaptive AI Technology
	b) Bot Protection: identify visitor behavior through analysis of technical and behavioral data.
☒ P, Q, **N** or I Notes: doesn’t talk to different levels of proofing	2. **Identity Proofing must have the ability to provide levels of proofing which will be directly tied to the constituent’s level of access.**
	1) Define various levels of id proofing
	2) Document Image Capture
	3) Close coupling with authentication
☒ P, Q, **N** or I Notes: just says supported, does say which technology or subcontractor	3. **Multi-factor authentication The system must support multi-factor authentication to protect against user impersonation and credential theft.**
☒ P, Q, **N** or I	4. **Risk-based factors The system must support risk-based factors and scores that are based on factors such as, but not limited to, device and location.**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: CarahSoft
DATE: 06032024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

Notes: does not call out device or location	
☒ P, Q, N or **I** Notes:	**5. Identity lifecycle management components The system must include the following identity lifecycle management components for risk-based critical applications not limited to end users but also for generic accounts and system/service accounts:**
	1) Identity Creation
	2) Identity provisioning
	3) Attribute maps
	4) Authentication (e.g., password policies and synchronization)

☒ P, Q, **N** or I Notes: Is only called out for Ping; but no other contractors or subcontractors	**6. Security event logging The system must log security information and events.**
	Security Information and Event Management (SIEM) – Splunk
	Cloud Services: Azure, AWS, Oracle, Google
☒ P, Q, **N** or I Notes:	**7. Security Certifications The system must comply too or have the following security certifications:**
Does not meet requirements	1) NIST 800-53
	2) FedRamp
	3) HIPAA

	4) SOC 2 Type II
	Note:
	IRS require a 45-day letter approval for new cloud solutions.
☒ P, Q, **N** or **I** Notes: Does not call out integration for all products	**8. SIEM (Splunk) integration The system must be able to integrate with the State of Maine Security Information and Event Monitoring (SIEM) Splunk for Security Operations Center operations.**
☐ P, Q, **N** or **I** Notes: is not specifically called out by technology or vendor	**9. Core constituent data. The system must maintain a central repository of basic (core) constituent data, that can be used by any SoM application to reduce data redundancy and outdated or inaccurate information while maintaining confidentiality.**
☐ P, Q, **N** or **I** Notes: no support evidence	**11. Data Management. The system must apply the Data Management Rules to the constituent profile data as per the SoM Data Management Policies.**
☐ P, Q, **N** or **I** Notes: no support evidence	**12. SOM Employee. The system must support multiple identities for SOM employees that work with the portal in a support role.**
	1) SOM Employee identity and credentials for supporting the application.
	2) Constituent identity and credentials to use the state services offered through the portal.

☒ P, Q, N or **I** Notes:	**13. APIs. The system must be able to connect to at least one agency application.**

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: CarahSoft
DATE: 06032024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

Trivir talks to this requirement with ping	
	Considerations:
	a) OpenID, OAuth, WS-Fed, SAML, LDAP, Active Directory, Application Programming Interfaces (APIs), Software Development
	b) Develop once and reuse often with other agencies would be ideal
☐ P, Q, **N** or I Notes: no supporting evidence	**14. User identification matching. The system must be able to match the identity of the portal user to the identity of the same user in the agency system.**
☐ P, Q, N or **I** Notes:	**15. Single sign-on. The system must support single sign-on to the agency application.**
☐ P, Q, **N** or I Notes: No supporting evidence	**16. Import user profile data from agency systems. The system must be able to import user data from different SoM applications to ensure offboarding happens in a timely manner, so that government resources are protected from fraud. (example: death records)**
☒ P, Q, **N** or I Notes:	**17. History logging.** 1) The system must log all actions taken by:
No supporting evidence	a) Constituents
	b) MaineIT support
	Including but not limited to:
	c) who made the change
	d) when the change was made
	e) what changed
☒ P, Q, N or **I** Notes:	**18. Reporting. The logging data (history) must be available for constituent and system dashboards and reporting in general.**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: CarahSoft
DATE: 06032024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, **N** or I Notes:	**19. Security Controls. The system must comply to the following security controls:**
No mention of how other vendors, technology or subcontractors other than pingone	1) DDOS Protections[WN1] ,
	2) OWASP Top 10
	a) Cross Site Scripting,
	b) SQL Injection,
	3) Authentication bypass,
	a) poorly authenticated APIs,
	b) Role based access controls,
	c) proper session control
	4) Real-time visibility,
	5) Anomalous behavior,
	6) User sign with geo-location tracking,
	Geo-blocking capabilities.
	Security controls must include Web Application Firewall [WN1]
☒ P, Q, **N** or I Notes:	**20. General System Requirements.** 1) Mobile Support with Native App; (iOS and Android)
Only mentions adobe, does not mention other vendors, technology or subcontractors	2) System availability: 24/7 with 4x1-hour outages per year
	3) Identity relationships must be tracked in the cloud infrastructure.
	4) Support responsive web and web browsers.

	a. Supports Windows, Chrome, and Macintosh operating systems
☒ P, Q, **N** or I Notes:	**21. Training and Support.** 1) Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
Does not call out all vendors and technology	2) MaineIT will require technical/administrator training. There will be initial training and on-going training as users are added.
	3) Have a continuous process to ensure constituents that may have run into issues setting up accounts can have help 24/7.
☒ P, Q, N or **I** Notes:	**22. Support Requirements** 1) The Bidder will provide support, and maintenance for the solution to begin immediately after receiving the State's official acceptance of the implemented solution.
	2) Support and maintenance will be provided for the terms and duration specified in the contract.
	3) The Bidder will address all questions and reported problems related to the technical and functional operation of the system.
	4) The Bidder must provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours: 8:00 a.m. to 5:00 p.m. Eastern Standard Time.
	5) As part of the maintenance agreement, the Bidder will make all product releases and upgrades available to the State at no additional charge.
	6) All release and upgrades shall be implemented and tested by the Bidder, outside of the normal operating hours of the State government.
	7) User testing shall occur during normal State business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State government.
☒ P, Q, **N** or I Notes: Does not call out all	**23. Hosting** Solution can comply with MaineIT remote hosting policies. a) Remote Hosting Policy http://maine.gov/oit/policies/RemoteHostingPolicy.pdf

vendors and technology	b) Hosting Customization Policy http://maine.gov/oit/policies/HostingCustomizationPolicy.pdf
☒ P, Q, **N** or I Notes: Does not call out all vendors and technology	**24. Disaster Recovery** Proposed Solution can comply with MaineIT security requirements and remote hosting requirements, without requiring waivers, before contract finalization.
	1) Maintaining an availability metric of ninety-nine-point nine percent (99.9%) of uptime
	2) Ensuring the capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six hours (i.e., maximum data loss cannot exceed six (6) hours);
	3) Ensuring a recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours;
	4) Ensuring the hosting environment provides adequate capacity to ensure that, under ethernet connectivity to the client device, data inquiry/lookup response is within three (3) seconds, and data modification response is within five (5) seconds;
	5) Providing the Department at least thirty (30) calendar day advance written notice of any material change in network operations or architecture;
	6) Ensuring any planned material change in network operations or architecture cannot be made without the prior written consent of the Department; and Outlining of all Service Level Agreements (SLAs) for technical support (the awarded Bidder shall be open to negotiation to ensure the SLAs meet the Department's needs

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

☒1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
P, N, Q, or **I** & Notes:

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: CarahSoft
DATE: 06032024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

☒1b) Detailed description of the technologies, software and / or hardware for each of the components.
P, **N**, Q, or **I** & Notes:
Does not call out the complete call solutions

☒1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.
P, **N**, Q, or **I** & Notes:
Does not go into detail

☒1d) Description of the overall platform and architecture of the proposed solution(s).
P, N, Q, or **I** & Notes:

☒1e) Description of any third-party software or partnerships required for the proposed Solution(s).
P, N, Q, or **I** & Notes:

☐2a) A detailed timeline and description of milestones, deliverables, tasks
P, **N,** Q, or I & Notes:
Not provided

☐2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period
P, **N**, Q, or I & Notes:
Not provided

☒2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
P, **N**, Q, or I & Notes:
Not fully flushed out for all components

☒2d) Average time to market for each component.
P, **N**, Q, or I & Notes:

Not provided

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. ☒Capture Constituent Identity and profile data.
   P, N, Q, or **I** & Notes:

b. ☒Provide identity provisioning and deprovisioning.
   P, **N**, Q, or I & Notes:
   doesn't give detail

c. ☒Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
   i. Identity Creation
   ii. Identity provisioning
   iii. Attribute maps
   iv. Authentication (e.g., password policies and synchronization)
      P, N, **Q**, or I & Notes:

d. ☒Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies.
   P, N, Q, or **I** & Notes:

e. ☒Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
   P, **N**, Q, or I & Notes: does not talk about how replication is prevented

f. ☒Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.
   P, N, Q, or **I** & Notes:

g. ☒Allow for multiple role selections for the following identities:
   i. Individual
   ii. Business Owner
   iii. Support multiple identities for State employees that work with the portal in a support role:

(a) SOM Employee identity and credentials for supporting the application.
(b) Constituent identity and credentials to use the state services offered through the portal.

iv. Multi role individual (Individual and Business Owner)
P, N, Q, or **I** & Notes:

h. ☒Have the ability to provide levels of proofing which will be directly tied to the Constituent's level of consent given.
P, **N**, Q, or I & Notes: does not provide detail

i. ☒Support multi-factor authentication to protect against user impersonation and credential theft.
P, N, Q, or **I** & Notes:

B.2. ☒The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.
P, **N**, Q, or I & Notes: doesn't talk to the citizen experience of being recommended a service based on services consumed

a. Disclosure and Consent Management

The desire of the State is to be as transparent as possible and respect the privacy of the individual interacting with the Constituents' Portal. Consent is a core tenant of maintaining the public trust in the Constituents' Portal and will be a foundational component of the architecture.

The Disclosure and Consent Management solution shall include:

i. ☐Granular consent management that encompasses the automated functions necessary to create, modify, revoke, and manage Constituent consents.
ii. ☐Allow users the ability to opt-in and opt-out of data sharing and services within the Constituents' portal.

iii. ☐Obtain user consent both in an interactive and set preference mode for a variety of transactions on the Portal.
iv. ☐Support administrative users' management of standard legal disclaimers and data classification for transactions.
v. ☐Highly configurable with version control and history tracking for consent language.
vi. ☐Ability for end user to access a retrievable log of granted consent and data usage on the portal derived from the consent.

P, **N**, Q, or I & Notes:
Doesnt talk about how the features of onetrust meet our needs and requirements

b. Recommendation Technology

The State is seeking options which, while maintaining individual privacy, will collect and analyze data about user interactions, behavior, and preferences. The expected outcome of this will be to provide insights and intelligence that help the State make informed decisions and improve Constituent experiences.

i. ☐From the user perspective, the portal should be able to make real-time recommendations for related services.
ii. ☐Data captured in this environment must be obfuscated, as to not allow any party to directly target or track the preferences of an individual or their usage of the portal.
iii. ☐Solution providers should discuss in detail their use, storage, destruction of metadata, and tracking technologies with emphasis on how their offering provides analytical insights while protecting the individual user privacy.

P, **N**, Q, or I & Notes:

c. Data Management

The State is seeking the ability for the portal's Constituent identity to be linked to records maintained by individual State agencies. The proposed solution will include:

i. ☐Capabilities to streamline the sharing of data between State systems, including
    i. The identity assurance level
    ii. Agency to user notifications
    iii. Verification of user consent

iv. Identity resolution
v. Data sharing between agencies.

ii. ☐Maintain a central repository of basic (core) Constituent data, that can be used by any State application to reduce data redundancy, and outdated or inaccurate information while maintaining confidentiality.
iii. ☐Ability to integrate with State applications using, OpenID, OAuth, Web Services Federation Protocol (WS-Fed), Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), Active Directory, Application Programming Interface (API) or equivalent protocols.
iv. ☐Ability to match the identity of the portal user to the identity of the same user in the Agency system.
v. ☐Log all actions taken by:
  i. Constituents
  ii. MaineIT Support, including:
    (a) Who made the change
    (b) When the change was made
    (c) What changed to and from
vi. ☐Logging data must be available for system dashboards and reporting.

P, **N**, Q, or I & Notes:

d. Customer Service

The State is seeking solution(s) to provide 24/7/365 customer service to Constituents regardless of their location or technical abilities.

i. ☐Support Constituents with personalized and timely assistance.
ii. ☐Provide the state options to support our Constituents across multiple channels including, but not limited to phone, email, chat, etc.

P, N, Q, or **I** & Notes: introduced new subcontractor;

C.1. General System

a. ☐Mobile support with native app (iOS and Android)
b. ☐System availability: 24/7 with a maximum of four (4) 1-hour outages per year
c. ☐Identity relationships must be tracked in the cloud infrastructure.
d. ☐Support responsive web and web browsers.
  i. ☐Supports Windows, Chrome, and Macintosh operating systems.

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: CarahSoft
DATE: 06032024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

P, **N**, Q, or I & Notes:
Doesn't specify which technology or subcontractor meet this requirement

C.2. ☒Compliance with MaineIT Policies & Standards

a. Architecture Compliance Policy
b. System and Services Acquisition Policy and Procedures (SA-1)
c. Application Deployment Certification Policy
d. Digital Accessibility Policy
e. Remote Hosting Policy
f. Data Exchange Policy
g. Information Security Policy
h. Access Control Policy (AC-1)
i. Access Control Procedures for Users (AC-2)
j. Risk Assessment Policy and Procedures (RA-1)
k. Vulnerability Scanning Procedure (RA-5)
l. Security Assessment and Authorization Policy and Procedures (CA-1)
m. System and Information Integrity Policy and Procedures (SI-1)
n. Configuration Management Policy (CM-1)
o. Web Standards

P, N, Q, or **I** & Notes:

C.3. Support and Maintenance

a. ☐Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State's official acceptance of the implemented solution.
P, **N**, Q, or I & Notes:
does not call out all vendors and technology

b. ☐Terms and duration of the support and maintenance will be specified in the contract.
P, **N**, Q, or I & Notes:
Does not specify

c. ☒All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
P, N, Q, or **I** & Notes:
does not call out all vendors and technology

d. ☐Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
P, **N**, Q, or I & Notes:
Is not stated

e. ☐All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
P, **N**, Q, or I & Notes:
Is not stated

f. ☐All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
P, **N**, Q, or I & Notes:
Is not stated

g. ☐User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
P, N, Q, or **I** & Notes:

4. Security

The proposed solutions must provide a robust security system that aligns with the States Security Policies, standards, and Processes, Including:

Comply with or have the following security certifications:

i. ☐National Institute of Standards and Technology (NIST) 800-53
ii. ☐FedRamp
iii. ☐Health Insurance Portability and Accountability Act (HIPAA)
iv. ☐SOC 2 Type II
v. ☐Comply to the following security controls:
vi. ☐DDOS Protections [WN1]
vii. ☐Open Web Application Security Project (OWASP) Top 10
viii. ☐Cross Site Scripting
ix. ☐Structured Query Language (SQL) Injection
x. ☐Authentication bypass
xi. ☐Poorly authenticated APIs
xii. ☐Role based access controls

xiii. ☐Proper session control
xiv. ☐Real-time visibility
xv. ☐Anomalous behavior
xvi. ☐User sign with geo-location tracking
xvii. ☐Geo-blocking capabilities.
xviii. ☐Web Application Firewall [WN1]
xix. ☐System security must include the following security components:
xx. ☐Account take over protections
xxi. ☐Account sign-in Protections
xxii. ☐Behavior detection and evaluation
xxiii. ☐Adaptive AI Technology
xxiv. ☐Bot Protection; identity visitor behavior through analysis, technical and behavioral data.
xxv. ☐The proposed solution must be able to integrate with the State Security Information and Event Monitoring (SIEM) Splunk. Ability to log security information and events.

P, **N**, Q, or **I** & Notes:

is not stated for all vendors, technology and subcontractors. Does not meet fedramp requirement

5. **Licensing**

☐The State is aware that multiple licensing options are available and will be required to support the proposed solution in its entirety. The State seeks bids which will provide the most cost-effective licensing approach. Bidders are required to provide a detail breakdown for the proposed licensing.

P, **N**, Q, or **I** & Notes:

No licensing information for any vendor or technology was provided

1. **Training and OCM (Organizational Change Management)**

   a. ☒Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
   b. ☒Training must include technical and administrator training, initial and ongoing as users are added.
   c. ☒Continuous process to ensure Constituents that may have run into issues setting up accounts have help 24/7.
   d. ☒Bidders shall guide the State in OCM engagement for the duration of

project planning, transition, and final implementation phase including:

  i. Designing and managing team structures with roles and responsibilities to facilitate automated program delivery, while noting any risks anticipated from the lack of readiness in the organization and staffing.
  ii. Ensure a successful transition for the integration of new processes and technology with stakeholders.
  iii. Organizational readiness assessment

P, N, Q, or **I** & Notes:

3. Disaster Recovery

a. ☐Availability of ninety-nine-point nine percent (99.9%) of uptime
b. ☐Capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six (6) hours (i.e., maximum data loss cannot exceed six (6) hours)
c. ☐Recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours.

P, **N**, Q, or I & Notes:

Is not provided for all vendor and technology components

4. Feature Enhancements

a. ☒The State is seeking two hundred and fifty (250) hours of time and material for each proposed technology (CIAM), Personalized Dashboard, Disclosure and Consent Management, Data Management, and Recommendation Technology) to allow for specifications and enhancements during the contract period.

P, N, Q, or **I** & Notes:

5. Project Management

a. ☐The State plans to have its own project manager however, the awarded Bidder must have a project manager that has the primary responsibility for executing the project management tasks associated with the project. The awarded Bidder will:
  i. Work in collaboration with the State's Project Manager
  ii. Align with State Project Management processes and practices.

b. ☐Manage the implementation, executing all activities, tasks, deliverables and resource needs, both state and awarded Bidder.
c. ☐Track project status including managing and tracking all project risks, issues and decisions.
d. ☐Track and report status of deliverables and project status
e. ☐The awarded Bidder will provide their approach for project management and administration services including:
   i. Project Management Methodology
   ii. Project Governance
   iii. Resource Allocation and Schedule Management approach
   iv. Communication Management Approach including status reporting and document repository management.
   v. Risk and Issue Management Methodology
   vi. Change Management Methodology
   vii. Quality Management Methodology

P, **N**, Q, or I & Notes:

Does not talk about all vendor and technology components

D. Value Added Options (Other)

☒Bidders shall provide value added optional services to address relevant matters that have not been anticipated in this RFP but contribute to successful implementation of the proposed solutions, as well as any technology or services that will reduce risk to the project's quality and continuity. The value-added technology and services will not be included in the evaluation process but may be added during the contract negotiations.

P, N, Q, or **I** & Notes:

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: CarahSoft
DATE: 04 June 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: MaineIT

Section I – Preliminary Information (No points – Eligibility Requirements)

(File #1 App. A, B, C)
☒Done – Pass/Fail by Procurement & RFP Coordinator

Section II Organization Qualifications and Experience

(File #2 – App. D, E + other areas that have no Appendix number but are part of File #2)

1. Overview of the Organization (App. D)

☒Bidders must include three examples of projects which demonstrate their experience and expertise in performing these services as well as highlighting the Bidder's stated qualifications and skills.
N: Weak response

Statement of qualifications

☒Client name, contact person, Ph#, email.

Contract history with the state may be considered in rating proposals even if not provided by the bidder.
N: Contact details NOT provided (w/ the exception of one isolated name: Stephanie Goychman, Data Protection Officer, City of Neuilly sur Seine)
P: Contract history w/ the State
N: The OK example does NOT include Identity Management
N: The IL example does NOT include Identity Management
N: Services Australia example. The 25 M Australians owning a MyGov account does suggest Identity Management. But, no Identity Management product is mentioned. Therefore, scope is unclear.
P: State of Utah Trivir example does include Identity Management
P: Fairfax County Public Schools Trivir example does include Identity Management
P: State of New Hampshire Trivir example does include Identity Management
P: America First Federal Credit Union example does include Identity Management
P: Adobe Coca Cola example does include Personalized Dashboard
N: Adobe Dick's Sporting Goods example does NOT prove anything relevant
P: Adobe TSB example does include Recommendations
P: Adobe City of Neuilly sur Seine example does include Consent Management
N: Publicis Sapient PA example NOT relevant
N: Publicis Sapient Heathrow example NOT relevant
N: Publicis Sapient "Large Hotel Chain" example NOT relevant

N: Publicis Sapient LA Transport System example NOT relevant

2. **Subcontractors (App. E)**
   ☒If subcontractors are to be used, Bidders must provide the name, address, phone number, contact person, and a brief description of the subcontractors' organizational capacity and qualifications.
   Business name, contact person, address, ph#, email.
   N: Some data provided in a haphazard manner in different parts of the submission, but definitely NOT in the manner asked for

3. **Organizational Chart (No Appendix)**
   ☒Bidders must provide an organizational chart. The organizational chart must include the project being proposed. Each position must be identified by position title and corresponding to the personnel job descriptions.
   N: Not really an org-chart. Just a list of position titles.

4. **Litigation (No App.)**
   ☒Bidders must attach a list of all current litigation in which the Bidder is named and a list of all closed cases that have closed within the past five (5) years in which the Bidder paid the claimant either as part of a settlement or by decree. For each, list the entity bringing suit, the complaint, the accusation, amount, and outcome.
   P: Adequate response

5. **Financial Viability (No App.)**
   ☒Bidders must provide a current copy of their Dun & Bradstreet Business Information Report Snapshot.
   P: Strong response

6. **Licensure/Certification (No App.)**
   ☒Bidders *may* provide documentation of any applicable licensure/certification or specific credentials that are related to providing the proposed services of the RFP.
   P: Adequate response.

7. **Certificate of Insurance (No App.)**
   ☒Bidders must provide a certificate of insurance on a standard ACORD form (or the equivalent) evidencing the Bidder's general liability, professional liability and any other relevant liability insurance policies that might be associated with the proposed services.
   P: Includes $5 M Cyber Liability

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: CarahSoft
DATE: 04 June 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: MaineIT

Section III - Proposed Services

(File #3 – App. F, G, H)

1. Technical Assessment (App. F)

☒Done

2. Services to be Provided (App. G)

Note: on App. G Detailed Technical and Functional Requirements Excel spreadsheet, a tab is labeled User Stories. No response is required for Tab 3; these were provided to bidders for clarity and understanding of the expected journey a Constituent will experience.

☒ *N: Weak response* *N: No explanation* *N:No Evidence*	**1. System security components System security must include the following security components:**
	1) Account Take Over Protections
	a) Account Sign-in Protections
	a) Account Sign-in Protections
	a) Adaptive AI Technology
	b) Bot Protection: identify visitor behavior through analysis of technical and behavioral data.
☒ *P: Strong response*	**2. Identity Proofing must have the ability to provide levels of proofing which will be directly tied to the constituent's level of access.**
	1) Define various levels of id proofing
	2) Document Image Capture
	3) Close coupling with authentication
☒ *P: Strong reseponse*	**3. Multi-factor authentication The system must support multi-factor authentication to protect against user impersonation and credential theft.**
☒ *P: Strong response*	**4. Risk-based factors The system must support risk-based factors and scores that are based on factors such as, but not limited to, device and location.**

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: CarahSoft
DATE: 04 June 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: MaineIT

☒ *P: Strong response*	**5. Identity lifecycle management components The system must include the following identity lifecycle management components for risk-based critical applications not limited to end users but also for generic accounts and system/service accounts:**
	1) Identity Creation
	2) Identity provisioning
	3) Attribute maps
	4) Authentication (e.g., password policies and synchronization)
☒ *N: No explanation* *N: No evidence*	**6. Security event logging The system must log security information and events.**
	Security Information and Event Management (SIEM) – Splunk
	Cloud Services: Azure, AWS, Oracle, Google
☒ *N: Impossible to determine which products are covered*	**7. Security Certifications The system must comply too or have the following security certifications:**
	1) NIST 800-53
	2) FedRamp
	3) HIPAA
	4) SOC 2 Type II
	Note:
	IRS require a 45-day letter approval for new cloud solutions.
☒ *N: No explanation*	**8. SIEM (Splunk) integration The system must be able to integrate with the State of Maine Security Information and Event Monitoring (SIEM) Splunk for Security Operations Center operations.**

N: No evidence	
☒ *N: No explanation* *N: No evidence*	**9. Core constituent data. The system must maintain a central repository of basic (core) constituent data, that can be used by any SoM application to reduce data redundancy and outdated or inaccurate information while maintaining confidentiality.**
☒ *N: No explanation* *N: No evidence*	**11. Data Management. The system must apply the Data Management Rules to the constituent profile data as per the SoM Data Management Policies.**
☒ *N: No explanation* *N: No evidence*	**12. SOM Employee. The system must support multiple identities for SOM employees that work with the portal in a support role.**
	1) SOM Employee identity and credentials for supporting the application.
	2) Constituent identity and credentials to use the state services offered through the portal.
☒ *N: No explanation* *N: No evidence*	**13. APIs. The system must be able to connect to at least one agency application.**
	Considerations:
	a) OpenID, OAuth, WS-Fed, SAML, LDAP, Active Directory, Application Programming Interfaces (APIs), Software Development
	b) Develop once and reuse often with other agencies would be ideal
☒ *N: No explanation* *N: No evidence*	**14. User identification matching. The system must be able to match the identity of the portal user to the identity of the same user in the agency system.**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: CarahSoft
DATE: 04 June 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: MaineIT

☒ *N: No explanation* *N: No evidence*	**15. Single sign-on. The system must support single sign-on to the agency application.**
☒ *N: No explanation* *N: No evidence*	**16. Import user profile data from agency systems. The system must be able to import user data from different SoM applications to ensure offboarding happens in a timely manner, so that government resources are protected from fraud. (example: death records)**
☒ *N: No explanation* *N: No evidence*	**17. History logging.** 1) The system must log all actions taken by:
	a) Constituents
	b) MaineIT support
	Including but not limited to:
	c) who made the change
	d) when the change was made
	e) what changed
☒ *N: No explanation* *N: No evidence*	**18. Reporting. The logging data (history) must be available for constituent and system dashboards and reporting in general.**
☒ *N: No explanation* *N: No evidence*	**19. Security Controls. The system must comply to the following security controls:**
	1) DDOS Protections[WN1] ,
	2) OWASP Top 10
	a) Cross Site Scripting,
	b) SQL Injection,
	3) Authentication bypass,

	a) poorly authenticated APIs,
	b) Role based access controls,
	c) proper session control
	4) Real-time visibility,
	5) Anomalous behavior,
	6) User sign with geo-location tracking,
	Geo-blocking capabilities.
	Security controls must include Web Application Firewall [WN1]
☒ *N: No explanation* *N: No evidence*	**20. General System Requirements.** 1) Mobile Support with Native App; (iOS and Android)
	2) System availability: 24/7 with 4x1-hour outages per year
	3) Identity relationships must be tracked in the cloud infrastructure.
	4) Support responsive web and web browsers.
	a. Supports Windows, Chrome, and Macintosh operating systems
☒ *N: No explanation* *N: No evidence*	**21. Training and Support.** 1) Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
	2) MaineIT will require technical/administrator training. There will be initial training and on-going training as users are added.
	3) Have a continuous process to ensure constituents that may have run into issues setting up accounts can have help 24/7.
☒ *N: No explanation* *N: No evidence*	**22. Support Requirements** 1) The Bidder will provide support, and maintenance for the solution to begin immediately after receiving the State's official acceptance of the implemented solution.

	2) Support and maintenance will be provided for the terms and duration specified in the contract.
	3) The Bidder will address all questions and reported problems related to the technical and functional operation of the system.
	4) The Bidder must provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours: 8:00 a.m. to 5:00 p.m. Eastern Standard Time.
	5) As part of the maintenance agreement, the Bidder will make all product releases and upgrades available to the State at no additional charge.
	6) All release and upgrades shall be implemented and tested by the Bidder, outside of the normal operating hours of the State government.
	7) User testing shall occur during normal State business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State government.
☒ *N: No explanation* *N: No evidence*	**23. Hosting** Solution can comply with MaineIT remote hosting policies. a) Remote Hosting Policy http://maine.gov/oit/policies/RemoteHostingPolicy.pdf b) Hosting Customization Policy http://maine.gov/oit/policies/HostingCustomizationPolicy.pdf
☒ *N: No explanation* *N: No evidence* *N: Partial with respect to #5*	**24. Disaster Recovery** Proposed Solution can comply with MaineIT security requirements and remote hosting requirements, without requiring waivers, before contract finalization.
	1) Maintaining an availability metric of ninety-nine-point nine percent (99.9%) of uptime
	2) Ensuring the capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six hours (i.e., maximum data loss cannot exceed six (6) hours);

	3) Ensuring a recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours;
	4) Ensuring the hosting environment provides adequate capacity to ensure that, under ethernet connectivity to the client device, data inquiry/lookup response is within three (3) seconds, and data modification response is within five (5) seconds;
	5) Providing the Department at least thirty (30) calendar day advance written notice of any material change in network operations or architecture;
	6) Ensuring any planned material change in network operations or architecture cannot be made without the prior written consent of the Department; and Outlining of all Service Level Agreements (SLAs) for technical support (the awarded Bidder shall be open to negotiation to ensure the SLAs meet the Department’s needs

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

☒1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
P: Strong response

☒1b) Detailed description of the technologies, software and / or hardware for each of the components.
P: Strong response

☒1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.
P: Strong response

☒1d) Description of the overall platform and architecture of the proposed solution(s).
P: Strong response

☒1e) Description of any third-party software or partnerships required for the proposed Solution(s).
P: Adequate response

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: CarahSoft
DATE: 04 June 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: MaineIT

☐2a) A detailed timeline and description of milestones, deliverables, tasks
N: NO response

☐2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period
N: NO response

☐2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
N: NO response

☐2d) Average time to market for each component.
N: NO response

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. ☒Capture Constituent Identity and profile data.
   P: Strong response

b. ☒Provide identity provisioning and deprovisioning.
   P: Strong response

c. ☒Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
   i. Identity Creation
   ii. Identity provisioning
   iii. Attribute maps
   iv. Authentication (e.g., password policies and synchronization)
      P: Strong response

d. ☒Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies.

P: Strong response

e. ☒Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
P: Adequate response

f. ☒Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.
P: Strong response

g. ☐Allow for multiple role selections for the following identities:
   i. Individual
   ii. Business Owner
   iii. Support multiple identities for State employees that work with the portal in a support role:
      (a) SOM Employee identity and credentials for supporting the application.
      (b) Constituent identity and credentials to use the state services offered through the portal.
   iv. Multi role individual (Individual and Business Owner)
N: NO response

h. ☐Have the ability to provide levels of proofing which will be directly tied to the Constituent's level of consent given.
N: NO response

i. ☒Support multi-factor authentication to protect against user impersonation and credential theft.
P: Adequate response

B.2. ☒The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.

P: Strong response

a. Disclosure and Consent Management

The desire of the State is to be as transparent as possible and respect the privacy of the individual interacting with the Constituents' Portal. Consent is a core tenant of maintaining the public trust in the Constituents' Portal and will be a foundational component of the architecture.

The Disclosure and Consent Management solution shall include:

i. ☒Granular consent management that encompasses the automated functions necessary to create, modify, revoke, and manage Constituent consents.
P: Adequate response

ii. ☒Allow users the ability to opt-in and opt-out of data sharing and services within the Constituents' portal.
P: Adequate response

iii. ☒Obtain user consent both in an interactive and set preference mode for a variety of transactions on the Portal.
P: Adequate response

iv. ☒Support administrative users' management of standard legal disclaimers and data classification for transactions.
P: Adequate response

v. ☒Highly configurable with version control and history tracking for consent language.
P: Adequate response

vi. ☒Ability for end user to access a retrievable log of granted consent and data usage on the portal derived from the consent.
P: Adequate response

b. Recommendation Technology

The State is seeking options which, while maintaining individual privacy, will collect and analyze data about user interactions, behavior, and preferences. The expected outcome of this will be to provide insights and intelligence that help the State make informed decisions and improve Constituent experiences.

i. ☒From the user perspective, the portal should be able to make real-time recommendations for related services.
P: Adequate response

ii. ☐Data captured in this environment must be obfuscated, as to not allow any party to directly target or track the preferences of an individual or their usage of the portal.
N: NO response

iii. ☐Solution providers should discuss in detail their use, storage, destruction of metadata, and tracking technologies with emphasis on how their offering provides analytical insights while protecting the individual user privacy.
N: NO response

c. Data Management
The State is seeking the ability for the portal's Constituent identity to be linked to records maintained by individual State agencies. The proposed solution will include:

i. ☒Capabilities to streamline the sharing of data between State systems, including
   i. The identity assurance level
   ii. Agency to user notifications
   iii. Verification of user consent
   iv. Identity resolution
   v. Data sharing between agencies.
   P: Adequate response

ii. ☐Maintain a central repository of basic (core) Constituent data, that can be used by any State application to reduce data redundancy, and outdated or inaccurate information while maintaining confidentiality.
N: NO response

iii. ☒Ability to integrate with State applications using, OpenID, OAuth, Web Services Federation Protocol (WS-Fed), Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), Active Directory, Application Programming Interface (API) or equivalent protocols.
P: Adequate response

iv. ☒Ability to match the identity of the portal user to the identity of the same

user in the Agency system.
P: Adequate response

v. ☐Log all actions taken by:
   i. Constituents
   ii. MaineIT Support, including:
      (a) Who made the change
      (b) When the change was made
      (c) What changed to and from

N: NO response

vi. ☒Logging data must be available for system dashboards and reporting.
N: Covers Ping, but NOT Adobe, NOT OneTrust

d. Customer Service

The State is seeking solution(s) to provide 24/7/365 customer service to Constituents regardless of their location or technical abilities.

   i. ☒Support Constituents with personalized and timely assistance.
   ii. ☒Provide the state options to support our Constituents across multiple channels including, but not limited to phone, email, chat, etc.

P: Strong response
Q: Was it included in the Cost Proposal?

C.1. General System

   a. ☒Mobile support with native app (iOS and Android)
   b. ☒System availability: 24/7 with a maximum of four (4) 1-hour outages per year
   c. ☒Identity relationships must be tracked in the cloud infrastructure.
   d. ☒Support responsive web and web browsers.
      i. ☒Supports Windows, Chrome, and Macintosh operating systems.

P: Weak responses

C.2. ☒Compliance with MaineIT Policies & Standards

   a. Architecture Compliance Policy
   b. System and Services Acquisition Policy and Procedures (SA-1)
   c. Application Deployment Certification Policy
   d. Digital Accessibility Policy

e. Remote Hosting Policy
f. Data Exchange Policy
g. Information Security Policy
h. Access Control Policy (AC-1)
i. Access Control Procedures for Users (AC-2)
j. Risk Assessment Policy and Procedures (RA-1)
k. Vulnerability Scanning Procedure (RA-5)
l. Security Assessment and Authorization Policy and Procedures (CA-1)
m. System and Information Integrity Policy and Procedures (SI-1)
n. Configuration Management Policy (CM-1)
o. Web Standards

N: Weak response

C.3. Support and Maintenance

a. ☒Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State's official acceptance of the implemented solution.
N: Weak response. Covers Adobe & Ping, NOT OneTrust

b. ☒Terms and duration of the support and maintenance will be specified in the contract.
N: Weak response. Covers Adobe & Ping, NOT OneTrust

c. ☒All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
N: Weak response. Covers Adobe & Ping, NOT OneTrust

d. ☒Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
N: Weak response. Covers Adobe & Ping, NOT OneTrust

e. ☒All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
N: Did NOT respond to this item

f. ☐All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.

N: NO response

g. ☒User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
N: Weak response. Covers Adobe & Ping, NOT OneTrust

4. Security

The proposed solutions must provide a robust security system that aligns with the States Security Policies, standards, and Processes, Including:

Comply with or have the following security certifications:

i. ☒National Institute of Standards and Technology (NIST) 800-53
ii. ☒FedRamp
iii. ☒Health Insurance Portability and Accountability Act (HIPAA)
iv. ☒SOC 2 Type II
v. ☒Comply to the following security controls:
vi. ☒DDOS Protections [WN1]
vii. ☒Open Web Application Security Project (OWASP) Top 10
viii. ☒Cross Site Scripting
ix. ☒Structured Query Language (SQL) Injection
x. ☒Authentication bypass
xi. ☒Poorly authenticated APIs
xii. ☒Role based access controls
xiii. ☒Proper session control
xiv. ☒Real-time visibility
xv. ☒Anomalous behavior
xvi. ☒User sign with geo-location tracking
xvii. ☒Geo-blocking capabilities.
xviii. ☒Web Application Firewall [WN1]
xix. ☒System security must include the following security components:
xx. ☒Account take over protections
xxi. ☒Account sign-in Protections
xxii. ☒Behavior detection and evaluation
xxiii. ☒Adaptive AI Technology
xxiv. ☒Bot Protection; identity visitor behavior through analysis, technical and behavioral data.

xxv. ☒The proposed solution must be able to integrate with the State Security Information and Event Monitoring (SIEM) Splunk. Ability to log security information and events.

N: Weak response. Covers Adobe & Ping, NOT OneTrust

5. Licensing

☒The State is aware that multiple licensing options are available and will be required to support the proposed solution in its entirety. The State seeks bids which will provide the most cost-effective licensing approach. Bidders are required to provide a detail breakdown for the proposed licensing.

Q: Refers to the Cost Proposal?

1. Training and OCM (Organizational Change Management)

a. ☒Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
b. ☒Training must include technical and administrator training, initial and ongoing as users are added.
c. ☒Continuous process to ensure Constituents that may have run into issues setting up accounts have help 24/7.
d. ☐Bidders shall guide the State in OCM engagement for the duration of project planning, transition, and final implementation phase including:
  i. Designing and managing team structures with roles and responsibilities to facilitate automated program delivery, while noting any risks anticipated from the lack of readiness in the organization and staffing.
  ii. Ensure a successful transition for the integration of new processes and technology with stakeholders.
  iii. Organizational readiness assessment

N: Did NOT respond to d
P: Otherwise, adequate response

3. Disaster Recovery

a. ☒Availability of ninety-nine-point nine percent (99.9%) of uptime
b. ☒Capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six (6) hours (i.e., maximum data loss cannot exceed six (6) hours)
c. ☒Recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours.

N: Did NOT respond to the specific requirements
N: Weak response. Nominally covered Ping, NOT Adobe, NOT OneTrust.

4. **Feature Enhancements**

a. ☒The State is seeking two hundred and fifty (250) hours of time and material for each proposed technology (CIAM), Personalized Dashboard, Disclosure and Consent Management, Data Management, and Recommendation Technology) to allow for specifications and enhancements during the contract period.
P: Adequate response

5. **Project Management**
   a. ☒The State plans to have its own project manager however, the awarded Bidder must have a project manager that has the primary responsibility for executing the project management tasks associated with the project. The awarded Bidder will:
      i. Work in collaboration with the State's Project Manager
      ii. Align with State Project Management processes and practices.
   b. ☒Manage the implementation, executing all activities, tasks, deliverables and resource needs, both state and awarded Bidder.
   c. ☒Track project status including managing and tracking all project risks, issues and decisions.
   d. ☒Track and report status of deliverables and project status
   e. ☐The awarded Bidder will provide their approach for project management and administration services including:
      i. Project Management Methodology
      ii. Project Governance
      iii. Resource Allocation and Schedule Management approach
      iv. Communication Management Approach including status reporting and document repository management.
      v. Risk and Issue Management Methodology
      vi. Change Management Methodology
      vii. Quality Management Methodology
   N: Did NOT address e
   N: Weak response

D. **Value Added Options (Other)**

☒Bidders shall provide value added optional services to address relevant matters that have not been anticipated in this RFP but contribute to successful implementation of the proposed solutions, as well as any technology or services that

will reduce risk to the project's quality and continuity. The value-added technology and services will not be included in the evaluation process but may be added during the contract negotiations.
P: Additional services from Publicis Sapient

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Carahsoft
DATE: 5/28/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

Section I – Preliminary Information (No points – Eligibility Requirements)

(File #1 App. A, B, C)
☒Done – Pass/Fail by Procurement & RFP Coordinator

Section II Organization Qualifications and Experience

(File #2 – App. D, E + other areas that have no Appendix number but are part of File #2)

1. Overview of the Organization (App. D)

☒Bidders must include three examples of projects which demonstrate their experience and expertise in performing these services as well as highlighting the Bidder's stated qualifications and skills. N – all three examples are blank in regard to contact information and the 6 areas check boxes. Pgs 53-54.

Statement of qualifications

☒Client name, contact person, Ph#, email.

Contract history with the state may be considered in rating proposals even if not provided by the bidder.

P, N, Q, or I & Notes:

Adobe: N - Did not include person, ph#, email. First example is OK and does not offer SSO. It's just links, no credentialing. Same for ILL. But Australia does have SSO – credentialing. This bidder is proposing a whole new Maine.gov portal, not a constituent portal. Pg. 14 – they talk about recommendations but do not speak to "consent." Pg. 18 – "new Maine citizen portal."

TriVir: N - Did not include person, ph#, email. Number of current employees is 28, but will be dedicating 44 to the project? Very vague/limited descriptions of project completed.Their projects do not check off the components, pg. 41, none has more then two checked off.

Publicis Sapient: N: I really have no idea what this company does outside of "spaghetti tech" and advancing the capabilities for facilitating the streamlined sharing of data between state systems, API, integration, cloud computing but no details at all.

2. Subcontractors (App. E)

☒If subcontractors are to be used, Bidders must provide the name, address, phone number, contact person, and a brief description of the subcontractors' organizational capacity and qualifications.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Carahsoft
DATE: 5/28/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

Business name, contact person, address, ph#, email.

P, N, Q, or I & Notes: take yo   P – did not see subcontractors listed.

3. **Organizational Chart (No Appendix)**

☐Bidders must provide an organizational chart. The organizational chart must include the project being proposed. Each position must be identified by position title and corresponding to the personnel job descriptions.

P, N, Q, or I & Notes: N – no org chart presented, just a bulleted list that is very vague. They referenced PING but provided no info about PING as a company.

4. **Litigation (No App.)**

☒Bidders must attach a list of all current litigation in which the Bidder is named and a list of all closed cases that have closed within the past five (5) years in which the Bidder paid the claimant either as part of a settlement or by decree. For each, list the entity bringing suit, the complaint, the accusation, amount, and outcome.

P, N, Q, or I & Notes: P

5. **Financial Viability (No App.)**

☒Bidders must provide a current copy of their Dun & Bradstreet Business Information Report Snapshot.

P, N, Q, or I - Notes: N – D&B not presented. Carahsoft's Dun and Bradstreet Number is 088365767. Please Note: Carahsoft does not provide Dun and Bradstreet with financial information because we are privately held, therefore, Dun and Bradstreet does not
issue reports on Carahsoft.

6. **Licensure/Certification (No App.)**

☒Bidders *may* provide documentation of any applicable licensure/certification or specific credentials that are related to providing the proposed services of the RFP.

P, N, Q, or I & Notes: N – went to link, could not find licensure/cert.

7. **Certificate of Insurance (No App.)**

☒Bidders must provide a certificate of insurance on a standard ACORD form (or the equivalent) evidencing the Bidder's general liability, professional liability and any other relevant liability insurance policies that might be associated with the proposed services.

P, N, Q, or I & Notes: P

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Carahsoft
DATE: 5/28/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

Section III - Proposed Services

(File #3 – App. F, G, H)

1. Technical Assessment (App. F)

☒Done

2. Services to be Provided (App. G)

Note: on App. G Detailed Technical and Functional Requirements Excel spreadsheet, a tab is labeled User Stories. No response is required for Tab 3; these were provided to bidders for clarity and understanding of the expected journey a Constituent will experience.

☒ P, Q, N or I Notes: P – bidder put Y in box.	**1. System security components System security must include the following security components:**
	1) Account Take Over Protections
	a) Account Sign-in Protections
	a) Account Sign-in Protections
	a) Adaptive AI Technology
	b) Bot Protection: identify visitor behavior through analysis of technical and behavioral data.
☒ P, Q, N or I Notes: Overall, 2 is N. N on 1) . located in the Ping Document - No numbers are referenced to match up with RFP	**2. Identity Proofing must have the ability to provide levels of proofing which will be directly tied to the constituent's level of access.**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Carahsoft
DATE: 5/28/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

numbers. Marketing jargon. 2) P 3) N - Ping Document - No numbers are referenced to match up with RFP numbers. Marketing jargon.	
	1) Define various levels of id proofing
	2) Document Image Capture
	3) Close coupling with authentication
☒ P, Q, N or I Notes: P	**3. Multi-factor authentication The system must support multi-factor authentication to protect against user impersonation and credential theft.**
☒ P, Q, N or I Notes: P	**4. Risk-based factors The system must support risk-based factors and scores that are based on factors such as, but not limited to, device and location.**
☒ P, Q, N or I Notes: N – much is located in the Ping Advan. Document- was not able to determine the details asked for in this item when looking at the	**5. Identity lifecycle management components The system must include the following identity lifecycle management components for risk-based critical applications not limited to end users but also for generic accounts and system/service accounts:**

section the bidder referenced.	
	1) Identity Creation
	2) Identity provisioning
	3) Attribute maps
	4) Authentication (e.g., password policies and synchronization)

☒ P, Q, N or I Notes: P – bidder put Y in box.	**6. Security event logging The system must log security information and events.**
	Security Information and Event Management (SIEM) – Splunk
	Cloud Services: Azure, AWS, Oracle, Google
☒ P, Q, N or I Notes: N overall based on their answers to each section as shown below	**7. Security Certifications The system must comply too or have the following security certifications:**
P	1) NIST 800-53
N	2) FedRamp

Y	3) HIPAA
Y	4) SOC 2 Type II
	Note:
	IRS require a 45-day letter approval for new cloud solutions.
☒ P, Q, N or I Notes: P – bidder put Y in box.	**8. SIEM (Splunk) integration The system must be able to integrate with the State of Maine Security Information and Event Monitoring (SIEM) Splunk for Security Operations Center operations.**
☒ P, Q, N or I Notes: P – bidder put Y in box.	**9. Core constituent data. The system must maintain a central repository of basic (core) constituent data, that can be used by any SoM application to reduce data redundancy and outdated or inaccurate information while maintaining confidentiality.**
☒ P, Q, N or I Notes: P – bidder put Y in box.	**11. Data Management. The system must apply the Data Management Rules to the constituent profile data as per the SoM Data Management Policies.**
☒ P, Q, N or I Notes: P – bidder put Y in box.	**12. SOM Employee. The system must support multiple identities for SOM employees that work with the portal in a support role.**

	1) SOM Employee identity and credentials for supporting the application.
	2) Constituent identity and credentials to use the state services offered through the portal.

☒ P, Q, N or I Notes: I – bidder put Y in box -no details.	**13. APIs. The system must be able to connect to at least one agency application.**
	Considerations:
	a) OpenID, OAuth, WS-Fed, SAML, LDAP, Active Directory, Application Programming Interfaces (APIs), Software Development
	b) Develop once and reuse often with other agencies would be ideal
☒ P, Q, N or I Notes: : I – bidder put Y in box -no details.	**14. User identification matching. The system must be able to match the identity of the portal user to the identity of the same user in the agency system.**
☒ P, Q, N or I Notes: : I – bidder put Y in box -no details.	**15. Single sign-on. The system must support single sign-on to the agency application.**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Carahsoft
DATE: 5/28/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes: : I – bidder put Y in box -no details.	**16. Import user profile data from agency systems. The system must be able to import user data from different SoM applications to ensure offboarding happens in a timely manner, so that government resources are protected from fraud. (example: death records)**
☒ P, Q, N or I Notes: : I – bidder put Y in box -no details.	**17. History logging.** 1) The system must log all actions taken by:
	a) Constituents
	b) MaineIT support
	Including but not limited to:
	c) who made the change
	d) when the change was made
	e) what changed
☒ P, Q, N or I Notes: : I – bidder put Y in box -no details.	**18. Reporting. The logging data (history) must be available for constituent and system dashboards and reporting in general.**
☒ P, Q, N or I Notes: : I – bidder put Y in	**19. Security Controls. The system must comply to the following security controls:**

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Carahsoft
DATE: 5/28/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

box -no details.	
	1) DDOS Protections[WN1] ,
	2) OWASP Top 10
	a) Cross Site Scripting,
	b) SQL Injection,
	3) Authentication bypass,
	a) poorly authenticated APIs,
	b) Role based access controls,
	c) proper session control
	4) Real-time visibility,
	5) Anomalous behavior,
	6) User sign with geo-location tracking,
	Geo-blocking capabilities.
	Security controls must include Web Application Firewall [WN1]
☒ P, Q, N or I Notes: I – bidder put Y in box -no details.	**20. General System Requirements.** 1) Mobile Support with Native App; (iOS and Android)
	2) System availability: 24/7 with 4x1-hour outages per year
	3) Identity relationships must be tracked in the cloud infrastructure.
	4) Support responsive web and web browsers.
	a. Supports Windows, Chrome, and Macintosh operating systems
☒ P, Q, N or I Notes: : I – bidder put Y in	**21. Training and Support.** 1) Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.

box -no details.	
	2) MaineIT will require technical/administrator training. There will be initial training and on-going training as users are added.
	3) Have a continuous process to ensure constituents that may have run into issues setting up accounts can have help 24/7.
☒ P, Q, N or I Notes: I – bidder put Y in box -no details.	**22. Support Requirements** 1) The Bidder will provide support, and maintenance for the solution to begin immediately after receiving the State's official acceptance of the implemented solution.
	2) Support and maintenance will be provided for the terms and duration specified in the contract.
	3) The Bidder will address all questions and reported problems related to the technical and functional operation of the system.
	4) The Bidder must provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours: 8:00 a.m. to 5:00 p.m. Eastern Standard Time.
	5) As part of the maintenance agreement, the Bidder will make all product releases and upgrades available to the State at no additional charge.
	6) All release and upgrades shall be implemented and tested by the Bidder, outside of the normal operating hours of the State government.
	7) User testing shall occur during normal State business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State government.
☒ P, Q, N or I Notes: : I – bidder	**23. Hosting** Solution can comply with MaineIT remote hosting policies. a) Remote Hosting Policy http://maine.gov/oit/policies/RemoteHostingPolicy.pdf b) Hosting Customization Policy http://maine.gov/oit/policies/HostingCustomizationPolicy.pdf

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Carahsoft
DATE: 5/28/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

put Y in box -no details	
☒ P, Q, N or I Notes: N: bidder could only do partial in 5)	**24. Disaster Recovery** Proposed Solution can comply with MaineIT security requirements and remote hosting requirements, without requiring waivers, before contract finalization.
	1) Maintaining an availability metric of ninety-nine-point nine percent (99.9%) of uptime
	2) Ensuring the capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six hours (i.e., maximum data loss cannot exceed six (6) hours);
	3) Ensuring a recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours;
	4) Ensuring the hosting environment provides adequate capacity to ensure that, under ethernet connectivity to the client device, data inquiry/lookup response is within three (3) seconds, and data modification response is within five (5) seconds;
	5) Providing the Department at least thirty (30) calendar day advance written notice of any material change in network operations or architecture;
	6) Ensuring any planned material change in network operations or architecture cannot be made without the prior written consent of the Department; and Outlining of all Service Level Agreements (SLAs) for technical support (the awarded Bidder shall be open to negotiation to ensure the SLAs meet the Department's needs

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Carahsoft
DATE: 5/28/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

☒1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
P, N, Q, or I & Notes:
N – No Detailed description of anything. SSO listed as a Future Goal

☒1b) Detailed description of the technologies, software and / or hardware for each of the components.
P, N, Q, or I & Notes: N – No Detailed description of anything. Numbering in response does not match up to the areas asked for.

☒1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.
P, N, Q, or I & Notes: N – No Detailed description of anything. Numbering in response does not match up to the areas asked for.

☒1d) Description of the overall platform and architecture of the proposed solution(s).
P, N, Q, or I & Notes: N – No Detailed description of anything. Numbering in response does not match up to the areas asked for.

☒1e) Description of any third-party software or partnerships required for the proposed Solution(s).
P, N, Q, or I & Notes: N – No Detailed description of anything. Numbering in response does not match up to the areas asked for.

☒2a) A detailed timeline and description of milestones, deliverables, tasks
P, N, Q, or I & Notes: N – No Detailed description of anything. Numbering in response does not match up to the areas asked for.

☒2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period
P, N, Q, or I & Notes: N – Project Team not described. Lists three entities, one of which is DAFS Rep. Two others without asked for designations. Interestingly, this area lists SSO as part of the core configuration even though it is stated in last section that it is a future goal. No Detailed description of anything. Numbering in response does not match up to the areas asked for. “This plan does not include integrations to different applications now. We understand that those connections would be scoped during the discovery phase

and can impact the overall plan as we could consider a phased approach. This work plan assumes one go live date with core portal and functionality setup." This approach does not include what we have asked for in regard to a service being online.

☒2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
P, N, Q, or I & Notes: N – Based on answer above, this workplan does not include all components asked for such as an agency app actually being deployed.
☒2d) Average time to market for each component.
P, N, Q, or I & Notes: N – No Detailed description of anything. Numbering in response does not match up to the areas asked for.

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. ☒Capture Constituent Identity and profile data.
   P, N, Q, or I & Notes: N – very lengthy marking jargon for ID.me that speaks to all the security aspects and standards met, but no mention of the constituent identity or profile data gathering., The link to the Preverified flow for Maine does not work.
b. ☒Provide identity provisioning and deprovisioning.
   P, N, Q, or I & Notes: Q – I am unsure about this one. I did not see either provisioning or de referenced. However, they use the word provisioning under the next section. Hard to follow.
c. ☒Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
   i. Identity Creation
   ii. Identity provisioning
   iii. Attribute maps
   iv. Authentication (e.g., password policies and synchronization)
   P, N, Q, or I & Notes: N – no language on password policies
d. ☒Allow integration with applications across various State Agencies. More

specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies.
P, N, Q, or I & Notes: N – did not address.

e. ☒Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
P, N, Q, or I & Notes: N – does not speak to integrating with SoM agencies, provided marking jargon around what ID.me offers.

f. ☒Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.
P, N, Q, or I & Notes: Q – A lot of language around security measures but no language around biometrics.

g. ☒Allow for multiple role selections for the following identities:
   i. Individual
   ii. Business Owner
   iii. Support multiple identities for State employees that work with the portal in a support role:
      (a) SOM Employee identity and credentials for supporting the application.
      (b) Constituent identity and credentials to use the state services offered through the portal.
   iv. Multi role individual (Individual and Business Owner)
   P, N, Q, or I & Notes: N – lists only two types of identities: Internal and external and did not go into detail on the identities SoM specifically asked for.

h. ☒Have the ability to provide levels of proofing which will be directly tied to the Constituent's level of consent given.
P, N, Q, or I & Notes: N – see review of section a above.

i. ☒Support multi-factor authentication to protect against user impersonation and credential theft.
P, N, Q, or I & Notes: N – lists marketing jargon for MFA and never mentions impersonation or credential theft.

B.2. ☒The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State

services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.
P, N, Q, or I & Notes: P

a. Disclosure and Consent Management

The desire of the State is to be as transparent as possible and respect the privacy of the individual interacting with the Constituents' Portal. Consent is a core tenant of maintaining the public trust in the Constituents' Portal and will be a foundational component of the architecture.

The Disclosure and Consent Management solution shall include:

☒Granular consent management that encompasses the automated functions necessary to create, modify, revoke, and manage Constituent consents. ☐Allow users the ability to opt-in and opt-out of data sharing and services within the Constituents' portal.

i. ☒Obtain user consent both in an interactive and set preference mode for a variety of transactions on the Portal.

☐Support administrative users' management of standard legal disclaimers and data classification for transactions. Q – this is concerning, on pg. 36: Users may also opt-in or opt-out to receiving tailored marketing content from shop.ID.me, ID.me's affiliate marketplace. ID.me's branded relationship with end users enables us to market programs like unemployment insurance to our network of 125M users, more than 18M of whom have opted into our marketing emails. This unique feature enables us to drive additional customer traffic to agency partners from our already ID validated user base, contributing to greater conversion rates.

ii.

☒Highly configurable with version control and history tracking for consent language. N – does not speak to version control.

iii. ☒Ability for end user to access a retrievable log of granted consent and data usage on the portal derived from the consent. P

P, N, Q, or I & Notes: N - overall

b. Recommendation Technology

The State is seeking options which, while maintaining individual privacy, will collect and analyze data about user interactions, behavior, and preferences. The expected outcome of this will be to provide insights and intelligence that help the State make informed decisions and improve Constituent experiences.

i. ☒From the user perspective, the portal should be able to make real-time recommendations for related services.

☒Data captured in this environment must be obfuscated, as to not allow any party to directly target or track the preferences of an individual or their usage of the portal. I - ServiceNow offers data anonymization techniques to protect individual user identities. However, it's important to understand that complete anonymization might limit the effectiveness of the recommendation engine

ii.
iii. ☒Solution providers should discuss in detail their use, storage, destruction of metadata, and tracking technologies with emphasis on how their offering provides analytical insights while protecting the individual user privacy. N – not provided.

P, N, Q, or I & Notes: N – overall did not address all sections.

c. Data Management

The State is seeking the ability for the portal's Constituent identity to be linked to records maintained by individual State agencies. The proposed solution will include:

i. ☒Capabilities to streamline the sharing of data between State systems, including
    i. The identity assurance level
    ii. Agency to user notifications
    iii. Verification of user consent
    iv. Identity resolution
    v. Data sharing between agencies.
ii. ☒Maintain a central repository of basic (core) Constituent data, that can be used by any State application to reduce data redundancy, and outdated or inaccurate information while maintaining confidentiality.
iii. ☒Ability to integrate with State applications using, OpenID, OAuth, Web Services Federation Protocol (WS-Fed), Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), Active Directory, Application Programming Interface (API) or equivalent protocols.
iv. ☒Ability to match the identity of the portal user to the identity of the same user in the Agency system.
v. ☒Log all actions taken by:
    i. Constituents
    ii. MaineIT Support, including:
        (a) Who made the change

(b) When the change was made
(c) What changed to and from

vi. ☒Logging data must be available for system dashboards and reporting.

P, N, Q, or I & Notes: I - **t's important to note that configuring ServiceNow to meet these requirements might involve implementing additional plugins or customizations.** However, the core functionalities like data management, integration, and logging are all built into the platform.

d. Customer Service

The State is seeking solution(s) to provide 24/7/365 customer service to Constituents regardless of their location or technical abilities.

  i. ☒Support Constituents with personalized and timely assistance. N – not included in price
  ii. ☒Provide the state options to support our Constituents across multiple channels including, but not limited to phone, email, chat, etc. N – speaks to technical support not constituent, until last paragraph, as an additional offering.

P, N, Q, or I & Notes: N

C.1. General System

a. ☒Mobile support with native app (iOS and Android)
b. ☒System availability: 24/7 with a maximum of four (4) 1-hour outages per year
c. ☒Identity relationships must be tracked in the cloud infrastructure.
d. ☒Support responsive web and web browsers.
  i. ☒Supports Windows, Chrome, and Macintosh operating systems.

P, N, Q, or I & Notes: P

C.2. ☐Compliance with MaineIT Policies & Standards

a. Architecture Compliance Policy
b. System and Services Acquisition Policy and Procedures (SA-1)
c. Application Deployment Certification Policy
d. Digital Accessibility Policy
e. Remote Hosting Policy
f. Data Exchange Policy

g. Information Security Policy
h. Access Control Policy (AC-1)
i. Access Control Procedures for Users (AC-2)
j. Risk Assessment Policy and Procedures (RA-1)
k. Vulnerability Scanning Procedure (RA-5)
l. Security Assessment and Authorization Policy and Procedures (CA-1)
m. System and Information Integrity Policy and Procedures (SI-1)
n. Configuration Management Policy (CM-1)
o. Web Standards

P, N, Q, or I & Notes: N – did not speak to meeting SoM policy/procedural requirements.

C.3. Support and Maintenance

a. ☒Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State's official acceptance of the implemented solution.
P, N, Q, or I & Notes:

b. ☒Terms and duration of the support and maintenance will be specified in the contract.
P, N, Q, or I & Notes:

c. ☒All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
P, N, Q, or I & Notes:

d. ☒Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
P, N, Q, or I & Notes: N – through portal only

e. ☒All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
P, N, Q, or I & Notes:

f. ☒All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
P, N, Q, or I & Notes:

g. ☒User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
P, N, Q, or I & Notes: N – no phone number for support.

4. Security

The proposed solutions must provide a robust security system that aligns with the States Security Policies, standards, and Processes, Including:

Comply with or have the following security certifications:

i. ☐National Institute of Standards and Technology (NIST) 800-53
ii. ☐FedRamp
iii. ☐Health Insurance Portability and Accountability Act (HIPAA)
iv. ☐SOC 2 Type II
v. ☐Comply to the following security controls:
vi. ☐DDOS Protections [WN1]
vii. ☐Open Web Application Security Project (OWASP) Top 10
viii. ☐Cross Site Scripting
ix. ☐Structured Query Language (SQL) Injection
x. ☐Authentication bypass
xi. ☐Poorly authenticated APIs
xii. ☐Role based access controls
xiii. ☐Proper session control
xiv. ☐Real-time visibility
xv. ☐Anomalous behavior
xvi. ☐User sign with geo-location tracking
xvii. ☐Geo-blocking capabilities.
xviii. ☐Web Application Firewall [WN1]
xix. ☐System security must include the following security components:
xx. ☐Account take over protections
xxi. ☐Account sign-in Protections
xxii. ☐Behavior detection and evaluation
xxiii. ☐Adaptive AI Technology
xxiv. ☐Bot Protection; identity visitor behavior through analysis, technical and behavioral data.

xxv. ☐The proposed solution must be able to integrate with the State Security Information and Event Monitoring (SIEM) Splunk. Ability to log security information and events.

P, N, Q, or I & Notes: N – bidder did not address most of the items required.

5. Licensing

☒The State is aware that multiple licensing options are available and will be required to support the proposed solution in its entirety. The State seeks bids which will provide the most cost-effective licensing approach. Bidders are required to provide a detail breakdown for the proposed licensing.

P, N, Q, or I & Notes: N – included in cost proposal

1. Training and OCM (Organizational Change Management)

a. ☒Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
b. ☒Training must include technical and administrator training, initial and ongoing as users are added.
c. ☒Continuous process to ensure Constituents that may have run into issues setting up accounts have help 24/7.
d. ☒Bidders shall guide the State in OCM engagement for the duration of project planning, transition, and final implementation phase including:
    i. Designing and managing team structures with roles and responsibilities to facilitate automated program delivery, while noting any risks anticipated from the lack of readiness in the organization and staffing.
    ii. Ensure a successful transition for the integration of new processes and technology with stakeholders.
    iii. Organizational readiness assessment

P, N, Q, or I & Notes: N – did not address a., c

3. Disaster Recovery

a. ☒Availability of ninety-nine-point nine percent (99.9%) of uptime
b. ☒Capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six (6) hours (i.e., maximum data loss cannot exceed six (6) hours)

c. ☒Recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours.

P, N, Q, or I & Notes: N – did not address our specific needs - timelines.

4. Feature Enhancements

a. ☒The State is seeking two hundred and fifty (250) hours of time and material for each proposed technology (CIAM), Personalized Dashboard, Disclosure and Consent Management, Data Management, and Recommendation Technology) to allow for specifications and enhancements during the contract period.

P, N, Q, or I & Notes: N – bidder returned marketing jargon.

5. Project Management

a. ☒The State plans to have its own project manager however, the awarded Bidder must have a project manager that has the primary responsibility for executing the project management tasks associated with the project. The awarded Bidder will:
   i. Work in collaboration with the State's Project Manager
   ii. Align with State Project Management processes and practices.
b. ☒Manage the implementation, executing all activities, tasks, deliverables and resource needs, both state and awarded Bidder.
c. ☒Track project status including managing and tracking all project risks, issues and decisions.
d. ☒Track and report status of deliverables and project status
e. ☐The awarded Bidder will provide their approach for project management and administration services including:
   i. Project Management Methodology
   ii. Project Governance
   iii. Resource Allocation and Schedule Management approach
   iv. Communication Management Approach including status reporting and document repository management.
   v. Risk and Issue Management Methodology
   vi. Change Management Methodology
   vii. Quality Management Methodology

P, N, Q, or I & Notes: N – did not state they would work with our project manager. Re-presented aspects of the project timeline which were not asked for. Did not address governance or document management.

D. Value Added Options (Other)

☒Bidders shall provide value added optional services to address relevant matters that have not been anticipated in this RFP but contribute to successful implementation of the proposed solutions, as well as any technology or services that will reduce risk to the project's quality and continuity. The value-added technology and services will not be included in the evaluation process but may be added during the contract negotiations.

P, N, Q, or I & Notes: P

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Deloitte
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

Section I – Preliminary Information (No points – Eligibility Requirements)

(File #1 App. A, B, C)
☒Done – Pass/Fail by Procurement & RFP Coordinator

Section II Organization Qualifications and Experience

(File #2 – App. D, E + other areas that have no Appendix number but are part of File #2)

1. Overview of the Organization (App. D)

☒Bidders must include three examples of projects which demonstrate their experience and expertise in performing these services as well as highlighting the Bidder's stated qualifications and skills.

Statement of qualifications

☒Client name, contact person, Ph#, email.

Contract history with the state may be considered in rating proposals even if not provided by the bidder.
No client names or contacts, No indications they will be provided
P, N, Q, or I & Notes:

2. Subcontractors (App. E)

☒If subcontractors are to be used, Bidders must provide the name, address, phone number, contact person, and a brief description of the subcontractors' organizational capacity and qualifications.
Business name, contact person, address, ph#, email.
P, N, Q, or I & Notes:P none

3. Organizational Chart (No Appendix)

☒Bidders must provide an organizational chart. The organizational chart must include the project being proposed. Each position must be identified by position title and corresponding to the personnel job descriptions.
P, N, Q, or I & Notes:P

4. Litigation (No App.)

☒Bidders must attach a list of all current litigation in which the Bidder is named and a list of all closed cases that have closed within the past five (5) years in which the Bidder paid the claimant either as part of a settlement or by decree. For each, list the entity bringing suit, the complaint, the accusation, amount, and outcome.
P, N, Q, or I & Notes:Q **Written 3 years instead of 5 years**

5. **Financial Viability (No App.)**
☒Bidders must provide a current copy of their Dun & Bradstreet Business Information Report Snapshot.
P, N, Q, or I - Notes:Q not provided

6. **Licensure/Certification (No App.)**
☒Bidders *may* provide documentation of any applicable licensure/certification or specific credentials that are related to providing the proposed services of the RFP.
P, N, Q, or I & Notes:Not provided

7. **Certificate of Insurance (No App.)**
☒Bidders must provide a certificate of insurance on a standard ACORD form (or the equivalent) evidencing the Bidder's general liability, professional liability and any other relevant liability insurance policies that might be associated with the proposed services.
P, N, Q, or I & Notes:Not provided

Section III - Proposed Services

(File #3 – App. F, G, H)

1. **Technical Assessment (App. F)**
☒Done

2. **Services to be Provided (App. G)**

Note: on App. G Detailed Technical and Functional Requirements Excel spreadsheet, a tab is labeled User Stories. No response is required for Tab 3; these were provided to bidders for clarity and understanding of the expected journey a Constituent will experience.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Deloitte
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes:P	**1. System security components System security must include the following security components:**
	1) Account Take Over Protections
	a) Account Sign-in Protections
	a) Account Sign-in Protections
	a) Adaptive AI Technology
	b) Bot Protection: identify visitor behavior through analysis of technical and behavioral data.
☒ P, Q, N or I Notes: P	**2. Identity Proofing must have the ability to provide levels of proofing which will be directly tied to the constituent's level of access.**
	1) Define various levels of id proofing
	2) Document Image Capture
	3) Close coupling with authentication
☒ P, Q, N or I Notes: P	**3. Multi-factor authentication The system must support multi-factor authentication to protect against user impersonation and credential theft.**
☒ P, Q, N or I Notes: P	**4. Risk-based factors The system must support risk-based factors and scores that are based on factors such as, but not limited to, device and location.**
☒ P, Q, N or I Notes: P Missing a description of off boarding	**5. Identity lifecycle management components The system must include the following identity lifecycle management components for risk-based critical applications not limited to end users but also for generic accounts and system/service accounts:**
p	1) Identity Creation
P	2) Identity provisioning
P	3) Attribute maps
P	4) Authentication (e.g., password policies and synchronization)

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Deloitte
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes:P Assiumes State management of the aws env for Recommendations engine	**6. Security event logging The system must log security information and events.**
	Security Information and Event Management (SIEM) – Splunk
	Cloud Services: Azure, AWS, Oracle, Google
☒ P, Q, N or I Notes:P	**7. Security Certifications The system must comply too or have the following security certifications:**
comply	1) NIST 800-53
comply	2) FedRamp
comply	3) HIPAA
comply	4) SOC 2 Type II
	Note:
	IRS require a 45-day letter approval for new cloud solutions.
☒ P, Q, N or I Notes:P	**8. SIEM (Splunk) integration The system must be able to integrate with the State of Maine Security Information and Event Monitoring (SIEM) Splunk for Security Operations Center operations.**
☒ P, Q, N or I Notes:P	**9. Core constituent data. The system must maintain a central repository of basic (core) constituent data, that can be used by any SoM application to reduce data redundancy and outdated or inaccurate information while maintaining confidentiality.**
☒ P, Q, N or I Notes:P	**11. Data Management. The system must apply the Data Management Rules to the constituent profile data as per the SoM Data Management Policies.**
☒ P, Q, N or I Notes:p	**12. SOM Employee. The system must support multiple identities for SOM employees that work with the portal in a support role.**

	1) SOM Employee identity and credentials for supporting the application.
	2) Constituent identity and credentials to use the state services offered through the portal.

☒ P, Q, N or I Notes:p Only will do 1 application	**13. APIs. The system must be able to connect to at least one agency application.**
	Considerations:
	a) OpenID, OAuth, WS-Fed, SAML, LDAP, Active Directory, Application Programming Interfaces (APIs), Software Development
	b) Develop once and reuse often with other agencies would be ideal
☒ P, Q, N or I Notes:P	**14. User identification matching. The system must be able to match the identity of the portal user to the identity of the same user in the agency system.**
☒ P, Q, N or I Notes:P	**15. Single sign-on. The system must support single sign-on to the agency application.**
☒ P, Q, N or I Notes:P	**16. Import user profile data from agency systems. The system must be able to import user data from different SoM applications to ensure offboarding happens in a timely manner, so that government resources are protected from fraud. (example: death records)**
☒ P, Q, N or I Notes:P	**17. History logging.** 1) The system must log all actions taken by:
p	a) Constituents
P	b) MaineIT support
	Including but not limited to:
p	c) who made the change
P	d) when the change was made

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Deloitte
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

p	e) what changed
☒ P, Q, N or I Notes:Q. made available to Siem but doesn't say dashboard	**18. Reporting. The logging data (history) must be available for constituent and system dashboards and reporting in general.**
☐ P, Q, N or I Notes:P	**19. Security Controls. The system must comply to the following security controls:**
P	1) DDOS Protections[WN1] ,
P	2) OWASP Top 10
P	a) Cross Site Scripting,
P	b) SQL Injection,
P	3) Authentication bypass,
P	a) poorly authenticated APIs,
P	b) Role based access controls,
P	c) proper session control
P	4) Real-time visibility,
P	5) Anomalous behavior,
P	6) User sign with geo-location tracking,
P	Geo-blocking capabilities.
P	Security controls must include Web Application Firewall [WN1]
☒ P, Q, N or I Notes:P	**20. General System Requirements.** 1) Mobile Support with Native App; (iOS and Android)
P	2) System availability: 24/7 with 4x1-hour outages per year
P	3) Identity relationships must be tracked in the cloud infrastructure.
P	4) Support responsive web and web browsers.
P	a. Supports Windows, Chrome, and Macintosh operating systems

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Deloitte
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes:P	**21. Training and Support.** 1) Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
P- 1 admin for okta per contract year	2) MaineIT will require technical/administrator training. There will be initial training and on-going training as users are added.
P:self service	3) Have a continuous process to ensure constituents that may have run into issues setting up accounts can have help 24/7.
☒ P, Q, N or I Notes:P	**22. Support Requirements** 1) The Bidder will provide support, and maintenance for the solution to begin immediately after receiving the State's official acceptance of the implemented solution.
P	2) Support and maintenance will be provided for the terms and duration specified in the contract.
P	3) The Bidder will address all questions and reported problems related to the technical and functional operation of the system.
Q and/or through the toll-free support number provided.	4) The Bidder must provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours: 8:00 a.m. to 5:00 p.m. Eastern Standard Time.
Q Product enhancements not included	5) As part of the maintenance agreement, the Bidder will make all product releases and upgrades available to the State at no additional charge.
P	6) All release and upgrades shall be implemented and tested by the Bidder, outside of the normal operating hours of the State government.
P	7) User testing shall occur during normal State business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State government.
☒ P, Q, N or I Notes:P	**23. Hosting** Solution can comply with MaineIT remote hosting policies. a) Remote Hosting Policy http://maine.gov/oit/policies/RemoteHostingPolicy.pdf b) Hosting Customization Policy http://maine.gov/oit/policies/HostingCustomizationPolicy.pdf

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Deloitte
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes:P	**24. Disaster Recovery** Proposed Solution can comply with MaineIT security requirements and remote hosting requirements, without requiring waivers, before contract finalization.
P	1) Maintaining an availability metric of ninety-nine-point nine percent (99.9%) of uptime
P	2) Ensuring the capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six hours (i.e., maximum data loss cannot exceed six (6) hours);
P	3) Ensuring a recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours;
P	4) Ensuring the hosting environment provides adequate capacity to ensure that, under ethernet connectivity to the client device, data inquiry/lookup response is within three (3) seconds, and data modification response is within five (5) seconds;
P	5) Providing the Department at least thirty (30) calendar day advance written notice of any material change in network operations or architecture;
P	6) Ensuring any planned material change in network operations or architecture cannot be made without the prior written consent of the Department; and Outlining of all Service Level Agreements (SLAs) for technical support (the awarded Bidder shall be open to negotiation to ensure the SLAs meet the Department's needs

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

☒1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
P, N, Q, or I & Notes:P

☒1b) Detailed description of the technologies, software and / or hardware for each of the components.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Deloitte
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

P, N, Q, or I & Notes:p

☒1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.
P, N, Q, or I & Notes:P

☒1d) Description of the overall platform and architecture of the proposed solution(s).
P, N, Q, or I & Notes:p

☐1e) Description of any third-party software or partnerships required for the proposed Solution(s).
P, N, Q, or I & Notes:

☒2a) A detailed timeline and description of milestones, deliverables, tasks
P, N, Q, or I & Notes:P

☐2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period
P, N, Q, or I & Notes:

☒2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
P, N, Q, or I & Notes:P

☒2d) Average time to market for each component.
P, N, Q, or I & Notes:P

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. ☒Capture Constituent Identity and profile data.
   P, N, Q, or I & Notes:p
b. ☒Provide identity provisioning and deprovisioning.
   P, N, Q, or I & Notes:Q nothing on deprovisioning
c. ☒Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
   i. Identity Creation
   ii. Identity provisioning
   iii. Attribute maps
   iv. Authentication (e.g., password policies and synchronization)
      P, N, Q, or I & Notes:p
d. ☒Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies.
   P, N, Q, or I & Notes:p
e. ☒Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
   P, N, Q, or I & Notes:P
f. ☒Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.
   P, N, Q, or I & Notes:P
g. ☒Allow for multiple role selections for the following identities:
   i. Individual
   ii. Business Owner
   iii. Support multiple identities for State employees that work with the portal in a support role:
      (a) SOM Employee identity and credentials for supporting the application.
      (b) Constituent identity and credentials to use the state services offered through the portal.
   iv. Multi role individual (Individual and Business Owner)
      P, N, Q, or I & Notes:P

h. ☒Have the ability to provide levels of proofing which will be directly tied to the Constituent's level of consent given.
   P, N, Q, or I & Notes:P
i. ☒Support multi-factor authentication to protect against user impersonation and credential theft.
   P, N, Q, or I & Notes:p

B.2. ☒The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.
P, N, Q, or I & Notes:P

a. Disclosure and Consent Management

The desire of the State is to be as transparent as possible and respect the privacy of the individual interacting with the Constituents' Portal. Consent is a core tenant of maintaining the public trust in the Constituents' Portal and will be a foundational component of the architecture.

The Disclosure and Consent Management solution shall include:

i. ☒Granular consent management that encompasses the automated functions necessary to create, modify, revoke, and manage Constituent consents.
ii. ☒Allow users the ability to opt-in and opt-out of data sharing and services within the Constituents' portal.
iii. ☒Obtain user consent both in an interactive and set preference mode for a variety of transactions on the Portal.
iv. ☒Support administrative users' management of standard legal disclaimers and data classification for transactions.
v. ☒Highly configurable with version control and history tracking for consent language.

vi. ☒Ability for end user to access a retrievable log of granted consent and data usage on the portal derived from the consent.

P, N, Q, or I & Notes:

b. Recommendation Technology

The State is seeking options which, while maintaining individual privacy, will collect and analyze data about user interactions, behavior, and preferences. The expected outcome of this will be to provide insights and intelligence that help the State make informed decisions and improve Constituent experiences.

i. ☒From the user perspective, the portal should be able to make real-time recommendations for related services.
ii. ☐Data captured in this environment must be obfuscated, as to not allow any party to directly target or track the preferences of an individual or their usage of the portal.
iii. ☐Solution providers should discuss in detail their use, storage, destruction of metadata, and tracking technologies with emphasis on how their offering provides analytical insights while protecting the individual user privacy.

P, N, Q, or I & Notes:Q Nothing about data obfuscation or storage /destruction of meta data

c. Data Management

The State is seeking the ability for the portal's Constituent identity to be linked to records maintained by individual State agencies. The proposed solution will include:

i. ☒Capabilities to streamline the sharing of data between State systems, including
    i. The identity assurance level
    ii. Agency to user notifications
    iii. Verification of user consent
    iv. Identity resolution
    v. Data sharing between agencies.
ii. ☒Maintain a central repository of basic (core) Constituent data, that can be used by any State application to reduce data redundancy, and outdated or inaccurate information while maintaining confidentiality.
iii. ☒Ability to integrate with State applications using, OpenID, OAuth, Web Services Federation Protocol (WS-Fed), Security Assertion Markup

Language (SAML), Lightweight Directory Access Protocol (LDAP), Active Directory, Application Programming Interface (API) or equivalent protocols.

iv. ☒Ability to match the identity of the portal user to the identity of the same user in the Agency system.
v. ☒Log all actions taken by:
   i. Constituents
   ii. MaineIT Support, including:
      (a) Who made the change
      (b) When the change was made
      (c) What changed to and from
vi. ☒Logging data must be available for system dashboards and reporting.

P, N, Q, or I & Notes:P

d. Customer Service

The State is seeking solution(s) to provide 24/7/365 customer service to Constituents regardless of their location or technical abilities.

i. ☒Support Constituents with personalized and timely assistance.
ii. ☒Provide the state options to support our Constituents across multiple channels including, but not limited to phone, email, chat, etc.

P, N, Q, or I & Notes: P

C.1. General System

a. ☒Mobile support with native app (iOS and Android)
b. ☒System availability: 24/7 with a maximum of four (4) 1-hour outages per year
c. ☒Identity relationships must be tracked in the cloud infrastructure.
d. ☒Support responsive web and web browsers.
   i. ☒Supports Windows, Chrome, and Macintosh operating systems.

P, N, Q, or I & Notes:

C.2. ☒Compliance with MaineIT Policies & Standards

a. Architecture Compliance Policy
b. System and Services Acquisition Policy and Procedures (SA-1)
c. Application Deployment Certification Policy
d. Digital Accessibility Policy

e. Remote Hosting Policy
f. Data Exchange Policy
g. Information Security Policy
h. Access Control Policy (AC-1)
i. Access Control Procedures for Users (AC-2)
j. Risk Assessment Policy and Procedures (RA-1)
k. Vulnerability Scanning Procedure (RA-5)
l. Security Assessment and Authorization Policy and Procedures (CA-1)
m. System and Information Integrity Policy and Procedures (SI-1)
n. Configuration Management Policy (CM-1)
o. Web Standards

P, N, Q, or I & Notes:P

C.3. Support and Maintenance

a. ☒Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State’s official acceptance of the implemented solution.
P, N, Q, or I & Notes:P

b. ☒Terms and duration of the support and maintenance will be specified in the contract.
P, N, Q, or I & Notes:P

c. ☒All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
P, N, Q, or I & Notes:P

d. ☒Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
P, N, Q, or I & Notes:Q Doesn’;t say will provide toll free

e. ☒All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
P, N, Q, or I & Notes:P

f. ☒All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
P, N, Q, or I & Notes:P

g. ☒User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
P, N, Q, or I & Notes:P

4. Security

The proposed solutions must provide a robust security system that aligns with the States Security Policies, standards, and Processes, Including:

Comply with or have the following security certifications:

i. ☒National Institute of Standards and Technology (NIST) 800-53
ii. ☒FedRamp
iii. ☒Health Insurance Portability and Accountability Act (HIPAA)
iv. ☒SOC 2 Type II
v. ☒Comply to the following security controls:
vi. ☒DDOS Protections [WN1]
vii. ☒Open Web Application Security Project (OWASP) Top 10
viii. ☒Cross Site Scripting
ix. ☒Structured Query Language (SQL) Injection
x. ☒Authentication bypass
xi. ☒Poorly authenticated APIs
xii. ☒Role based access controls
xiii. ☒Proper session control
xiv. ☒Real-time visibility
xv. ☒Anomalous behavior
xvi. ☒User sign with geo-location tracking
xvii. ☒Geo-blocking capabilities.
xviii. ☒Web Application Firewall [WN1]
xix. ☒System security must include the following security components:
xx. ☒Account take over protections
xxi. ☒Account sign-in Protections
xxii. ☒Behavior detection and evaluation
xxiii. ☒Adaptive AI Technology
xxiv. ☒Bot Protection; identity visitor behavior through analysis, technical and behavioral data.

xxv. ☒The proposed solution must be able to integrate with the State Security Information and Event Monitoring (SIEM) Splunk. Ability to log security information and events.

P, N, Q, or I & Notes:

5. Licensing

☒The State is aware that multiple licensing options are available and will be required to support the proposed solution in its entirety. The State seeks bids which will provide the most cost-effective licensing approach. Bidders are required to provide a detail breakdown for the proposed licensing.

P, N, Q, or I & Notes:P

1. Training and OCM (Organizational Change Management)

a. ☒Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
b. ☒Training must include technical and administrator training, initial and ongoing as users are added.
c. ☒Continuous process to ensure Constituents that may have run into issues setting up accounts have help 24/7.
d. ☒Bidders shall guide the State in OCM engagement for the duration of project planning, transition, and final implementation phase including:
    i. Designing and managing team structures with roles and responsibilities to facilitate automated program delivery, while noting any risks anticipated from the lack of readiness in the organization and staffing.
    ii. Ensure a successful transition for the integration of new processes and technology with stakeholders.
    iii. Organizational readiness assessment

P, N, Q, or I & Notes:

3. Disaster Recovery

a. ☒Availability of ninety-nine-point nine percent (99.9%) of uptime
b. ☒Capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six (6) hours (i.e., maximum data loss cannot exceed six (6) hours)

c. ☒Recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours.

P, N, Q, or I & Notes:P

4. Feature Enhancements

a. ☒The State is seeking two hundred and fifty (250) hours of time and material for each proposed technology (CIAM), Personalized Dashboard, Disclosure and Consent Management, Data Management, and Recommendation Technology) to allow for specifications and enhancements during the contract period.

P, N, Q, or I & Notes:P

5. Project Management

a. ☒The State plans to have its own project manager however, the awarded Bidder must have a project manager that has the primary responsibility for executing the project management tasks associated with the project. The awarded Bidder will:
   i. Work in collaboration with the State's Project Manager
   ii. Align with State Project Management processes and practices.
b. ☒Manage the implementation, executing all activities, tasks, deliverables and resource needs, both state and awarded Bidder.
c. ☒Track project status including managing and tracking all project risks, issues and decisions.
d. ☒Track and report status of deliverables and project status
e. ☒The awarded Bidder will provide their approach for project management and administration services including:
   i. Project Management Methodology
   ii. Project Governance
   iii. Resource Allocation and Schedule Management approach
   iv. Communication Management Approach including status reporting and document repository management.
   v. Risk and Issue Management Methodology
   vi. Change Management Methodology
   vii. Quality Management Methodology

P, N, Q, or I & Notes:P

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Deloitte
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

D. Value Added Options (Other)

☒Bidders shall provide value added optional services to address relevant matters that have not been anticipated in this RFP but contribute to successful implementation of the proposed solutions, as well as any technology or services that will reduce risk to the project's quality and continuity. The value-added technology and services will not be included in the evaluation process but may be added during the contract negotiations.

P, N, Q, or I & Notes:Pn Digital wallet

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Deloitte
DATE: 6/5/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

Section I – Preliminary Information (No points – Eligibility Requirements)

(File #1 App. A, B, C)
☒Done – Pass/Fail by Procurement & RFP Coordinator

Section II Organization Qualifications and Experience

(File #2 – App. D, E + other areas that have no Appendix number but are part of File #2)

1. Overview of the Organization (App. D)

☐Bidders must include three examples of projects which demonstrate their experience and expertise in performing these services as well as highlighting the Bidder's stated qualifications and skills.

Statement of qualifications

☐Client name, contact person, Ph#, email.

Contract history with the state may be considered in rating proposals even if not provided by the bidder.

P, **N**, Q, or **I** & Notes:

No file 2 provided with contract information or reference projects. Some high level overview of what features they have helped with in other states in AppH but no reference detail provided

2. Subcontractors (App. E)

☒If subcontractors are to be used, Bidders must provide the name, address, phone number, contact person, and a brief description of the subcontractors' organizational capacity and qualifications.

Business name, contact person, address, ph#, email.

P, N, Q, or **I** & Notes:

No subcontractors noted

3. Organizational Chart (No Appendix)

☒Bidders must provide an organizational chart. The organizational chart must include the project being proposed. Each position must be identified by position title and corresponding to the personnel job descriptions.

P, N, Q, or **I** & Notes:

Very detailed org chart with named resources; photos and matching resumes/job descriptions

4. **Litigation (No App.)**
☐Bidders must attach a list of all current litigation in which the Bidder is named and a list of all closed cases that have closed within the past five (5) years in which the Bidder paid the claimant either as part of a settlement or by decree. For each, list the entity bringing suit, the complaint, the accusation, amount, and outcome.
P, **N**, Q, or I & Notes:
No formal documentation provided stating current litigation status

5. **Financial Viability (No App.)**
☐Bidders must provide a current copy of their Dun & Bradstreet Business Information Report Snapshot.
P, **N**, Q, or I - Notes:
No formal documentation provided for financial viability

6. **Licensure/Certification (No App.)**
☐Bidders *may* provide documentation of any applicable licensure/certification or specific credentials that are related to providing the proposed services of the RFP.
P, N, Q, or I & Notes:
N/A

7. **Certificate of Insurance (No App.)**
☐Bidders must provide a certificate of insurance on a standard ACORD form (or the equivalent) evidencing the Bidder's general liability, professional liability and any other relevant liability insurance policies that might be associated with the proposed services.
P, **N**, Q, or I & Notes:

No formal documentation provided for Certificate of Insurance

Section III - Proposed Services

(File #3 – App. F, G, H)

1. **Technical Assessment (App. F)**
☒Done

2. **Services to be Provided (App. G)**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Deloitte
DATE: 6/5/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

Note: on App. G Detailed Technical and Functional Requirements Excel spreadsheet, a tab is labeled User Stories. No response is required for Tab 3; these were provided to bidders for clarity and understanding of the expected journey a Constituent will experience.

☒ P, Q, N or **I** Notes: no mention of how SSO integrates into solution	**1. System security components System security must include the following security components:**
	1) Account Take Over Protections
	a) Account Sign-in Protections
	a) Account Sign-in Protections
	a) Adaptive AI Technology
	b) Bot Protection: identify visitor behavior through analysis of technical and behavioral data.
☒ **P**, Q, N or I Notes: strong level of detail around proofing levels	**2. Identity Proofing must have the ability to provide levels of proofing which will be directly tied to the constituent's level of access.**
	1) Define various levels of id proofing
	2) Document Image Capture
	3) Close coupling with authentication
☒ **P**, Q, N or I Notes: All major MFA methods supported	**3. Multi-factor authentication The system must support multi-factor authentication to protect against user impersonation and credential theft.**
☒ P, Q, N or **I** Notes:	**4. Risk-based factors The system must support risk-based factors and scores that are based on factors such as, but not limited to, device and location.**
☒ P, Q, N or **I** Notes:	**5. Identity lifecycle management components The system must include the following identity lifecycle management components for risk-based critical applications not**

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Deloitte
DATE: 6/5/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

For ID: how do business and non-profit persona get provisioned	**limited to end users but also for generic accounts and system/service accounts:**
	1) Identity Creation
	2) Identity provisioning
	3) Attribute maps
	4) Authentication (e.g., password policies and synchronization)

☒ P, Q, N or **I** Notes: No mention of Socure logging	**6. Security event logging The system must log security information and events.**
	Security Information and Event Management (SIEM) – Splunk
	Cloud Services: Azure, **AWS**, Oracle, Google
☒ P, Q, N or **I** Notes:	**7. Security Certifications The system must comply too or have the following security certifications:**
Solid, but no evidence to support certifications	1) NIST 800-53
	2) FedRamp
	3) HIPAA
	4) SOC 2 Type II
	Note:
	IRS require a 45-day letter approval for new cloud solutions.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Deloitte
DATE: 6/5/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or **I** Notes: Again, no mention of Socure	**8. SIEM (Splunk) integration The system must be able to integrate with the State of Maine Security Information and Event Monitoring (SIEM) Splunk for Security Operations Center operations.**
☐ P, Q, **N** or I Notes: Does not explain how SoM applications consume data	**9. Core constituent data. The system must maintain a central repository of basic (core) constituent data, that can be used by any SoM application to reduce data redundancy and outdated or inaccurate information while maintaining confidentiality.**
☒ P, Q, N or **I** Notes:	**11. Data Management. The system must apply the Data Management Rules to the constituent profile data as per the SoM Data Management Policies.**
☒ P, Q, N or **I** Notes:	**12. SOM Employee. The system must support multiple identities for SOM employees that work with the portal in a support role.**
No mention of AD integration for SOM Employee persona	1) SOM Employee identity and credentials for supporting the application.
	2) Constituent identity and credentials to use the state services offered through the portal.

☒ **P**, Q, N or I Notes:	**13. APIs. The system must be able to connect to at least one agency application.**
	Considerations:
	a) OpenID, OAuth, WS-Fed, SAML, LDAP, Active Directory, Application Programming Interfaces (APIs), Software Development

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Deloitte
DATE: 6/5/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

	b) Develop once and reuse often with other agencies would be ideal
☒ P, Q, N or **I** Notes:	**14. User identification matching. The system must be able to match the identity of the portal user to the identity of the same user in the agency system.**
☒ P, Q, N or **I** Notes:	**15. Single sign-on. The system must support single sign-on to the agency application.**
☒ P, Q, **N** or I Notes: No detail provided around what happens with users data/records	**16. Import user profile data from agency systems. The system must be able to import user data from different SoM applications to ensure offboarding happens in a timely manner, so that government resources are protected from fraud. (example: death records)**
☒ **P**, Q, N or I Notes:	**17. History logging.** 1) The system must log all actions taken by:
Socure logging was detailed	a) Constituents
	b) MaineIT support
	Including but not limited to:
	c) who made the change
	d) when the change was made
	e) what changed
☐ P, Q, **N** or I Notes: Does not talking to reports for dashboards back to constituent	**18. Reporting. The logging data (history) must be available for constituent and system dashboards and reporting in general.**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Deloitte
DATE: 6/5/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

☒ **P**, Q, N or I Notes:	**19. Security Controls. The system must comply to the following security controls:**
	1) DDOS Protections[WN1] ,
	2) OWASP Top 10
	a) Cross Site Scripting,
	b) SQL Injection,
	3) Authentication bypass,
	a) poorly authenticated APIs,
	b) Role based access controls,
	c) proper session control
	4) Real-time visibility,
	5) Anomalous behavior,
	6) User sign with geo-location tracking,
	Geo-blocking capabilities.
	Security controls must include Web Application Firewall [WN1]
☒ P, Q, N or **I** Notes:	**20. General System Requirements.** 1) Mobile Support with Native App; (iOS and Android)
No mobile app for portal	2) System availability: 24/7 with 4x1-hour outages per year
	3) Identity relationships must be tracked in the cloud infrastructure.
	4) Support responsive web and web browsers.
	a. Supports Windows, Chrome, and Macintosh operating systems
☒ P, **Q**, N or I Notes:	**21. Training and Support.** 1) Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
Need more detail on continuous processes	2) MaineIT will require technical/administrator training. There will be initial training and on-going training as users are added.

	3) Have a continuous process to ensure constituents that may have run into issues setting up accounts can have help 24/7.
☒ P, Q, N or **I** Notes:	**22. Support Requirements** 1) The Bidder will provide support, and maintenance for the solution to begin immediately after receiving the State's official acceptance of the implemented solution.
	2) Support and maintenance will be provided for the terms and duration specified in the contract.
	3) The Bidder will address all questions and reported problems related to the technical and functional operation of the system.
Are they referencing constituent support?	4) The Bidder must provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours: 8:00 a.m. to 5:00 p.m. Eastern Standard Time.
For all products?	5) As part of the maintenance agreement, the Bidder will make all product releases and upgrades available to the State at no additional charge.
	6) All release and upgrades shall be implemented and tested by the Bidder, outside of the normal operating hours of the State government.
	7) User testing shall occur during normal State business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State government.
☒ P, **Q**, N or I Notes: salesforce needs to own all EULA	**23. Hosting** Solution can comply with MaineIT remote hosting policies. a) Remote Hosting Policy http://maine.gov/oit/policies/RemoteHostingPolicy.pdf b) Hosting Customization Policy http://maine.gov/oit/policies/HostingCustomizationPolicy.pdf
☒ P, Q, N or **I** Notes:	**24. Disaster Recovery** Proposed Solution can comply with MaineIT security requirements and remote hosting requirements, without requiring waivers, before contract finalization.
	1) Maintaining an availability metric of ninety-nine-point nine percent (99.9%) of uptime

Nothing noted for okta, socure	2) Ensuring the capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six hours (i.e., maximum data loss cannot exceed six (6) hours);
Nothing noted for okta socure	3) Ensuring a recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours;
	4) Ensuring the hosting environment provides adequate capacity to ensure that, under ethernet connectivity to the client device, data inquiry/lookup response is within three (3) seconds, and data modification response is within five (5) seconds;
What happens if they can't meet	5) Providing the Department at least thirty (30) calendar day advance written notice of any material change in network operations or architecture;
	6) Ensuring any planned material change in network operations or architecture cannot be made without the prior written consent of the Department; and Outlining of all Service Level Agreements (SLAs) for technical support (the awarded Bidder shall be open to negotiation to ensure the SLAs meet the Department's needs

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

☒1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
P, N, Q, or I & Notes:

☒1b) Detailed description of the technologies, software and / or hardware for each of the components.
P**,** N, Q, or **I** & Notes:
Google/AWS – recommendation engine

☒1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.

P, N, Q, or I & Notes:
Good table breaking products and services down to CP components

☒1d) Description of the overall platform and architecture of the proposed solution(s).
P, N, Q, or **I** & Notes:
Diagram doesn't show where aws as recommendation engine but Google; appG talks AWS

☒1e) Description of any third-party software or partnerships required for the proposed Solution(s).
P, N, Q, or **I** & Notes:

☒2a) A detailed timeline and description of milestones, deliverables, tasks
P, N, Q, or I & Notes:
Detailed timeline and project plan included

☒2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period
P, N, Q, or **I** & Notes:
Resource plan with vendor staff, resume and r&r included; however no mention of resourcing needs from the state side

☒2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
P, N, Q, or I & Notes:
Detailed timeline and project plan included

☒2d) Average time to market for each component.
P, N, Q, or I & Notes:

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture.

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Deloitte
DATE: 6/5/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. ☒Capture Constituent Identity and profile data.
   P, N, Q, or **I** & Notes: completed by okta
b. ☒Provide identity provisioning and deprovisioning.
   P, N, Q, or **I** & Notes: completed by okta
c. ☒Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
   i. Identity Creation
   ii. Identity provisioning
   iii. Attribute maps
   iv. Authentication (e.g., password policies and synchronization)
      P, N, Q, or **I** & Notes:
d. ☒Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies.
   P, N, Q, or **I** & Notes:
e. ☒Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
   P, N, Q, or **I** & Notes: how does it handle dups?
f. ☒Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.
   P, N, Q, or **I** & Notes: okta supported
g. ☒Allow for multiple role selections for the following identities:
   i. Individual
   ii. Business Owner
   iii. Support multiple identities for State employees that work with the portal in a support role:
      (a) SOM Employee identity and credentials for supporting the application.
      (b) Constituent identity and credentials to use the state services offered through the portal.
   iv. Multi role individual (Individual and Business Owner)
      P, N, Q, or **I** & Notes: can I move internally from persona to persona

h. ☒Have the ability to provide levels of proofing which will be directly tied to the Constituent's level of consent given.
   P, N, Q, or I & Notes: strong levels provided by socure

i. ☒Support multi-factor authentication to protect against user impersonation and credential theft.
   P, N, Q, or **I** & Notes:

B.2. ☒The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.
P, **N**, Q, or I & Notes:
Talks to recommendations of services but not a dashboard of current services in use by a constituent

a. Disclosure and Consent Management

The desire of the State is to be as transparent as possible and respect the privacy of the individual interacting with the Constituents' Portal. Consent is a core tenant of maintaining the public trust in the Constituents' Portal and will be a foundational component of the architecture.

The Disclosure and Consent Management solution shall include:

i. ☒Granular consent management that encompasses the automated functions necessary to create, modify, revoke, and manage Constituent consents.
ii. ☒Allow users the ability to opt-in and opt-out of data sharing and services within the Constituents' portal.
iii. ☒Obtain user consent both in an interactive and set preference mode for a variety of transactions on the Portal.
iv. ☒Support administrative users' management of standard legal disclaimers and data classification for transactions.
v. ☒Highly configurable with version control and history tracking for consent

language.

vi. ☒Ability for end user to access a retrievable log of granted consent and data usage on the portal derived from the consent.

P, N, Q, or I & Notes:

b. Recommendation Technology

The State is seeking options which, while maintaining individual privacy, will collect and analyze data about user interactions, behavior, and preferences. The expected outcome of this will be to provide insights and intelligence that help the State make informed decisions and improve Constituent experiences.

i. ☒From the user perspective, the portal should be able to make real-time recommendations for related services.
ii. ☐Data captured in this environment must be obfuscated, as to not allow any party to directly target or track the preferences of an individual or their usage of the portal.
iii. ☒Solution providers should discuss in detail their use, storage, destruction of metadata, and tracking technologies with emphasis on how their offering provides analytical insights while protecting the individual user privacy.

P, **N**, Q, or I & Notes:
Needs clarity; call out archetypes and AIRS taxonomy, but they aren't in the flow – does this match bullet 2

c. Data Management

The State is seeking the ability for the portal's Constituent identity to be linked to records maintained by individual State agencies. The proposed solution will include:

i. ☒Capabilities to streamline the sharing of data between State systems, including
    i. The identity assurance level
    ii. Agency to user notifications
    iii. Verification of user consent
    iv. Identity resolution
    v. Data sharing between agencies.
ii. ☒Maintain a central repository of basic (core) Constituent data, that can be used by any State application to reduce data redundancy, and outdated or

inaccurate information while maintaining confidentiality.

iii. ☒Ability to integrate with State applications using, OpenID, OAuth, Web Services Federation Protocol (WS-Fed), Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), Active Directory, Application Programming Interface (API) or equivalent protocols.
iv. ☒Ability to match the identity of the portal user to the identity of the same user in the Agency system.
v. ☒Log all actions taken by:
   i. Constituents
   ii. MaineIT Support, including:
      (a) Who made the change
      (b) When the change was made
      (c) What changed to and from
vi. ☒Logging data must be available for system dashboards and reporting.

P, N, Q, or I & Notes:

d. Customer Service

The State is seeking solution(s) to provide 24/7/365 customer service to Constituents regardless of their location or technical abilities.

i. ☒Support Constituents with personalized and timely assistance.
ii. ☒Provide the state options to support our Constituents across multiple channels including, but not limited to phone, email, chat, etc.

P, N, Q, or I & Notes:

C.1. General System

a. ☐Mobile support with native app (iOS and Android)
b. ☒System availability: 24/7 with a maximum of four (4) 1-hour outages per year
c. ☒Identity relationships must be tracked in the cloud infrastructure.
d. ☒Support responsive web and web browsers.
   i. ☒Supports Windows, Chrome, and Macintosh operating systems.

P, N, Q, or **I** & Notes:

No mobile native app – mobile first ux

C.2. ☒Compliance with MaineIT Policies & Standards

a. Architecture Compliance Policy
b. System and Services Acquisition Policy and Procedures (SA-1)
c. Application Deployment Certification Policy
d. Digital Accessibility Policy
e. Remote Hosting Policy
f. Data Exchange Policy
g. Information Security Policy
h. Access Control Policy (AC-1)
i. Access Control Procedures for Users (AC-2)
j. Risk Assessment Policy and Procedures (RA-1)
k. Vulnerability Scanning Procedure (RA-5)
l. Security Assessment and Authorization Policy and Procedures (CA-1)
m. System and Information Integrity Policy and Procedures (SI-1)
n. Configuration Management Policy (CM-1)
o. Web Standards

P, N, Q, or **I** & Notes:

C.3. Support and Maintenance

a. ☒Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State's official acceptance of the implemented solution.
   P, N, Q, or I & Notes:
b. ☒Terms and duration of the support and maintenance will be specified in the contract.
   P, N, Q, or I & Notes:

c. ☒All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
   P, N, Q, or I & Notes:
d. ☒Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
   P, N, Q, or I & Notes:
e. ☒All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
   P, N, Q, or **I** & Notes: no mention of okta, salesforce or socure updates

f. ☒All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
P, N, Q, or I & Notes:

g. ☒User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
P, N, Q, or I & Notes:

4. Security

The proposed solutions must provide a robust security system that aligns with the States Security Policies, standards, and Processes, Including:

Comply with or have the following security certifications:

i. ☒National Institute of Standards and Technology (NIST) 800-53
ii. ☒FedRamp
iii. ☒Health Insurance Portability and Accountability Act (HIPAA)
iv. ☒SOC 2 Type II
v. ☐Comply to the following security controls:
vi. ☒DDOS Protections [WN1]
vii. ☒Open Web Application Security Project (OWASP) Top 10
viii. ☒Cross Site Scripting
ix. ☒Structured Query Language (SQL) Injection
x. ☒Authentication bypass
xi. ☒Poorly authenticated APIs
xii. ☒Role based access controls
xiii. ☒Proper session control
xiv. ☒Real-time visibility
xv. ☒Anomalous behavior
xvi. ☒User sign with geo-location tracking
xvii. ☒Geo-blocking capabilities.
xviii. ☒Web Application Firewall [WN1]
xix. ☐System security must include the following security components:
xx. ☒Account take over protections
xxi. ☒Account sign-in Protections
xxii. ☒Behavior detection and evaluation
xxiii. ☒Adaptive AI Technology

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Deloitte
DATE: 6/5/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

xxiv. ☒Bot Protection; identity visitor behavior through analysis, technical and behavioral data.
xxv. ☒The proposed solution must be able to integrate with the State Security Information and Event Monitoring (SIEM) Splunk. Ability to log security information and events.

P, N, Q, or **I** & Notes:

5. Licensing

☒The State is aware that multiple licensing options are available and will be required to support the proposed solution in its entirety. The State seeks bids which will provide the most cost-effective licensing approach. Bidders are required to provide a detail breakdown for the proposed licensing.

P, N, Q, or **I** & Notes: makes assumptions about our current environment and tooling

1. Training and OCM (Organizational Change Management)

a. ☒Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
b. ☒Training must include technical and administrator training, initial and ongoing as users are added.
c. ☒Continuous process to ensure Constituents that may have run into issues setting up accounts have help 24/7.
d. ☒Bidders shall guide the State in OCM engagement for the duration of project planning, transition, and final implementation phase including:
   i. Designing and managing team structures with roles and responsibilities to facilitate automated program delivery, while noting any risks anticipated from the lack of readiness in the organization and staffing.
   ii. Ensure a successful transition for the integration of new processes and technology with stakeholders.
   iii. Organizational readiness assessment

P, N, Q, or **I** & Notes:
No live instructor led training

3. Disaster Recovery

a. ☒Availability of ninety-nine-point nine percent (99.9%) of uptime
b. ☒Capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six (6) hours (i.e., maximum data loss cannot exceed six (6) hours)
c. ☒Recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours.

P, **N**, Q, or I & Notes:

Does not specifically call out rpo and rto

4. **Feature Enhancements**

a. ☒The State is seeking two hundred and fifty (250) hours of time and material for each proposed technology (CIAM), Personalized Dashboard, Disclosure and Consent Management, Data Management, and Recommendation Technology) to allow for specifications and enhancements during the contract period.

P, N, Q, or I & Notes:

5. **Project Management**

a. ☒The State plans to have its own project manager however, the awarded Bidder must have a project manager that has the primary responsibility for executing the project management tasks associated with the project. The awarded Bidder will:
    i. Work in collaboration with the State's Project Manager
    ii. Align with State Project Management processes and practices.
b. ☒Manage the implementation, executing all activities, tasks, deliverables and resource needs, both state and awarded Bidder.
c. ☒Track project status including managing and tracking all project risks, issues and decisions.
d. ☒Track and report status of deliverables and project status
e. ☒The awarded Bidder will provide their approach for project management and administration services including:
    i. Project Management Methodology
    ii. Project Governance
    iii. Resource Allocation and Schedule Management approach
    iv. Communication Management Approach including status reporting and document repository management.

v. Risk and Issue Management Methodology
vi. Change Management Methodology
vii. Quality Management Methodology

P, N, Q, or I & Notes:

D. Value Added Options (Other)

☒Bidders shall provide value added optional services to address relevant matters that have not been anticipated in this RFP but contribute to successful implementation of the proposed solutions, as well as any technology or services that will reduce risk to the project’s quality and continuity. The value-added technology and services will not be included in the evaluation process but may be added during the contract negotiations.

P, N, Q, or **I** & Notes:

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Deloitte
DATE: 05 June 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: MaineIT

Section I – Preliminary Information (No points – Eligibility Requirements)

(File #1 App. A, B, C)
☒Done – Pass/Fail by Procurement & RFP Coordinator

Section II Organization Qualifications and Experience

(File #2 – App. D, E + other areas that have no Appendix number but are part of File #2)

1. **Overview of the Organization (App. D)**
   ☒Bidders must include three examples of projects which demonstrate their experience and expertise in performing these services as well as highlighting the Bidder's stated qualifications and skills.
   N: Sort-of responded as part of Appendix H
   P: Mentioned five states w/ somewhat relevant portfolios: TX, KY, MI, CT, & CO

   Statement of qualifications
   ☐Client name, contact person, Ph#, email.
   Contract history with the state may be considered in rating proposals even if not provided by the bidder.
   N: NO response
   P: Contract history w/ the State

2. **Subcontractors (App. E)**
   ☐If subcontractors are to be used, Bidders must provide the name, address, phone number, contact person, and a brief description of the subcontractors' organizational capacity and qualifications.
   Business name, contact person, address, ph#, email.
   N: NO response

3. **Organizational Chart (No Appendix)**
   ☒Bidders must provide an organizational chart. The organizational chart must include the project being proposed. Each position must be identified by position title and corresponding to the personnel job descriptions.
   P: Strong response

4. **Litigation (No App.)**
   ☐Bidders must attach a list of all current litigation in which the Bidder is named and a list of all closed cases that have closed within the past five (5) years in which the

Bidder paid the claimant either as part of a settlement or by decree. For each, list the entity bringing suit, the complaint, the accusation, amount, and outcome.
N: NO response

5. **Financial Viability (No App.)**
☐Bidders must provide a current copy of their Dun & Bradstreet Business Information Report Snapshot.
N: NO response

6. **Licensure/Certification (No App.)**
☐Bidders *may* provide documentation of any applicable licensure/certification or specific credentials that are related to providing the proposed services of the RFP.
N: NO response

7. **Certificate of Insurance (No App.)**
☐Bidders must provide a certificate of insurance on a standard ACORD form (or the equivalent) evidencing the Bidder's general liability, professional liability and any other relevant liability insurance policies that might be associated with the proposed services.
N: NO response

Section III - Proposed Services

(File #3 – App. F, G, H)

1. **Technical Assessment (App. F)**
☒Done

2. **Services to be Provided (App. G)**

Note: on App. G Detailed Technical and Functional Requirements Excel spreadsheet, a tab is labeled User Stories. No response is required for Tab 3; these were provided to bidders for clarity and understanding of the expected journey a Constituent will experience.

☒ *P: Strong response*	**1. System security components System security must include the following security components:**
	1) Account Take Over Protections
	a) Account Sign-in Protections
	a) Account Sign-in Protections

	a) Adaptive AI Technology
	b) Bot Protection: identify visitor behavior through analysis of technical and behavioral data.
☒ *P: Strong response*	**2. Identity Proofing must have the ability to provide levels of proofing which will be directly tied to the constituent's level of access.**
	1) Define various levels of id proofing
	2) Document Image Capture
	3) Close coupling with authentication
☒ *P: Strong response*	**3. Multi-factor authentication The system must support multi-factor authentication to protect against user impersonation and credential theft.**
☒ *P: Strong response*	**4. Risk-based factors The system must support risk-based factors and scores that are based on factors such as, but not limited to, device and location.**
☒ *P: Strong response*	**5. Identity lifecycle management components The system must include the following identity lifecycle management components for risk-based critical applications not limited to end users but also for generic accounts and system/service accounts:**
	1) Identity Creation
	2) Identity provisioning
	3) Attribute maps
	4) Authentication (e.g., password policies and synchronization)
☒ *P: Strong response*	**6. Security event logging The system must log security information and events.**
	Security Information and Event Management (SIEM) – Splunk
	Cloud Services: Azure, AWS, Oracle, Google
☒ *N: Weak response.*	**7. Security Certifications The system must comply too or have the following security certifications:**

Covered Okta, but NOT Salesforce, NOT Socure ID+. *P: Did ack the IRS 45-day notice.*	
	1) NIST 800-53
	2) FedRamp
	3) HIPAA
	4) SOC 2 Type II
	Note:
	IRS require a 45-day letter approval for new cloud solutions.
☒ *P: Strong response*	**8. SIEM (Splunk) integration The system must be able to integrate with the State of Maine Security Information and Event Monitoring (SIEM) Splunk for Security Operations Center operations.**
☒ *P: Strong response*	**9. Core constituent data. The system must maintain a central repository of basic (core) constituent data, that can be used by any SoM application to reduce data redundancy and outdated or inaccurate information while maintaining confidentiality.**
☒ *P: Strong response*	**11. Data Management. The system must apply the Data Management Rules to the constituent profile data as per the SoM Data Management Policies.**
☒ *P: Strong response*	**12. SOM Employee. The system must support multiple identities for SOM employees that work with the portal in a support role.**
	1) SOM Employee identity and credentials for supporting the application.
	2) Constituent identity and credentials to use the state services offered through the portal.
☒ *P: Strong response*	**13. APIs. The system must be able to connect to at least one agency application.**

	Considerations:
	a) OpenID, OAuth, WS-Fed, SAML, LDAP, Active Directory, Application Programming Interfaces (APIs), Software Development
	b) Develop once and reuse often with other agencies would be ideal
☒ *P: Adequate response*	**14. User identification matching. The system must be able to match the identity of the portal user to the identity of the same user in the agency system.**
☒ *P: Strong response*	**15. Single sign-on. The system must support single sign-on to the agency application.**
☒ *P: Adequate response*	**16. Import user profile data from agency systems. The system must be able to import user data from different SoM applications to ensure offboarding happens in a timely manner, so that government resources are protected from fraud. (example: death records)**
☒ *P: Adequate response (More coverage of Salesforce & Okta. Less coverage of Socure ID+)*	**17. History logging.** 1) The system must log all actions taken by:
	a) Constituents
	b) MaineIT support
	Including but not limited to:
	c) who made the change
	d) when the change was made
	e) what changed
☒ *P: Adequate response*	**18. Reporting. The logging data (history) must be available for constituent and system dashboards and reporting in general.**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Deloitte
DATE: 05 June 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: MaineIT

☒ *P: Adequate response (More coverage of Salesforce & Okta. Less coverage of Socure ID+)*	**19. Security Controls. The system must comply to the following security controls:**
	1) DDOS Protections[WN1] ,
	2) OWASP Top 10
	a) Cross Site Scripting,
	b) SQL Injection,
	3) Authentication bypass,
	a) poorly authenticated APIs,
	b) Role based access controls,
	c) proper session control
	4) Real-time visibility,
	5) Anomalous behavior,
	6) User sign with geo-location tracking,
	Geo-blocking capabilities.
	Security controls must include Web Application Firewall [WN1]
☒ *P: Strong response*	**20. General System Requirements.** 1) Mobile Support with Native App; (iOS and Android)
	2) System availability: 24/7 with 4x1-hour outages per year
	3) Identity relationships must be tracked in the cloud infrastructure.
	4) Support responsive web and web browsers.
	a. Supports Windows, Chrome, and Macintosh operating systems
☒ *N: Weak response (Covers Okta,*	**21. Training and Support.** 1) Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.

NOT Salesforce, NOT Socure ID+)	
	2) MaineIT will require technical/administrator training. There will be initial training and on-going training as users are added.
	3) Have a continuous process to ensure constituents that may have run into issues setting up accounts can have help 24/7.
☒ *P: Strong response*	**22. Support Requirements** 1) The Bidder will provide support, and maintenance for the solution to begin immediately after receiving the State's official acceptance of the implemented solution.
	2) Support and maintenance will be provided for the terms and duration specified in the contract.
	3) The Bidder will address all questions and reported problems related to the technical and functional operation of the system.
	4) The Bidder must provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours: 8:00 a.m. to 5:00 p.m. Eastern Standard Time.
	5) As part of the maintenance agreement, the Bidder will make all product releases and upgrades available to the State at no additional charge.
	6) All release and upgrades shall be implemented and tested by the Bidder, outside of the normal operating hours of the State government.
	7) User testing shall occur during normal State business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State government.
☒ *N: Weak response. No mention of the actual products (Salesforce,*	**23. Hosting** Solution can comply with MaineIT remote hosting policies. a) Remote Hosting Policy http://maine.gov/oit/policies/RemoteHostingPolicy.pdf b) Hosting Customization Policy http://maine.gov/oit/policies/HostingCustomizationPolicy.pdf

Okta, Socure ID+)	
☒ *P: Adequate response*	**24. Disaster Recovery** Proposed Solution can comply with MaineIT security requirements and remote hosting requirements, without requiring waivers, before contract finalization.
	1) Maintaining an availability metric of ninety-nine-point nine percent (99.9%) of uptime
	2) Ensuring the capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six hours (i.e., maximum data loss cannot exceed six (6) hours);
	3) Ensuring a recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours;
	4) Ensuring the hosting environment provides adequate capacity to ensure that, under ethernet connectivity to the client device, data inquiry/lookup response is within three (3) seconds, and data modification response is within five (5) seconds;
	5) Providing the Department at least thirty (30) calendar day advance written notice of any material change in network operations or architecture;
	6) Ensuring any planned material change in network operations or architecture cannot be made without the prior written consent of the Department; and Outlining of all Service Level Agreements (SLAs) for technical support (the awarded Bidder shall be open to negotiation to ensure the SLAs meet the Department's needs

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

☒1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
P: Strong response

☒1b) Detailed description of the technologies, software and / or hardware for each of the components.
P: Strong response

☒1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.
P: Strong response

☒1d) Description of the overall platform and architecture of the proposed solution(s).
P: Strong response

☒1e) Description of any third-party software or partnerships required for the proposed Solution(s).
P: Strong response

☒2a) A detailed timeline and description of milestones, deliverables, tasks
P: Strong response

☒2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period
P: Strong response

☒2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
P: Strong response

☒2d) Average time to market for each component.
N: This item was NOT addressed

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. ☒Capture Constituent Identity and profile data.
   P: Strong response

b. ☒Provide identity provisioning and deprovisioning.
   P: Strong response

c. ☒Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
   i. Identity Creation
   ii. Identity provisioning
   iii. Attribute maps
   iv. Authentication (e.g., password policies and synchronization)
      P: Strong response

d. ☒Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies.
   P: Strong response

e. ☒Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
   P: Strong response

f. ☒Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.
   P: Strong response

g. ☒Allow for multiple role selections for the following identities:
   i. Individual
   ii. Business Owner
   iii. Support multiple identities for State employees that work with the portal in a support role:
      (a) SOM Employee identity and credentials for supporting the application.
      (b) Constituent identity and credentials to use the state services offered through the portal.
   iv. Multi role individual (Individual and Business Owner)
   P: Strong response

h. ☒Have the ability to provide levels of proofing which will be directly tied to the Constituent's level of consent given.
   P: Strong response

i. ☒Support multi-factor authentication to protect against user impersonation and credential theft.
P: Strong response

B.2. ☒The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.
P: Strong response

a. Disclosure and Consent Management
The desire of the State is to be as transparent as possible and respect the privacy of the individual interacting with the Constituents' Portal. Consent is a core tenant of maintaining the public trust in the Constituents' Portal and will be a foundational component of the architecture.
The Disclosure and Consent Management solution shall include:

i. ☒Granular consent management that encompasses the automated functions necessary to create, modify, revoke, and manage Constituent consents.
P: Adequate response

ii. ☒Allow users the ability to opt-in and opt-out of data sharing and services within the Constituents' portal.
P: Adequate response

iii. ☒Obtain user consent both in an interactive and set preference mode for a variety of transactions on the Portal.
P: Adequate response

iv. ☒Support administrative users' management of standard legal disclaimers and data classification for transactions.
P: Adequate response

v. ☒Highly configurable with version control and history tracking for consent

language.
P: Adequate response

vi. ☒Ability for end user to access a retrievable log of granted consent and data usage on the portal derived from the consent.
P: Adequate response

b. Recommendation Technology

The State is seeking options which, while maintaining individual privacy, will collect and analyze data about user interactions, behavior, and preferences. The expected outcome of this will be to provide insights and intelligence that help the State make informed decisions and improve Constituent experiences.

i. ☒From the user perspective, the portal should be able to make real-time recommendations for related services.
P: Strong response

ii. ☐Data captured in this environment must be obfuscated, as to not allow any party to directly target or track the preferences of an individual or their usage of the portal.
N: NO response

iii. ☐Solution providers should discuss in detail their use, storage, destruction of metadata, and tracking technologies with emphasis on how their offering provides analytical insights while protecting the individual user privacy.
N: NO response

c. Data Management

The State is seeking the ability for the portal's Constituent identity to be linked to records maintained by individual State agencies. The proposed solution will include:

i. ☒Capabilities to streamline the sharing of data between State systems, including
    i. The identity assurance level
    ii. Agency to user notifications
    iii. Verification of user consent
    iv. Identity resolution
    v. Data sharing between agencies.
P: Strong response

ii. ☒Maintain a central repository of basic (core) Constituent data, that can be used by any State application to reduce data redundancy, and outdated or inaccurate information while maintaining confidentiality.
N: Strong response

iii. ☒Ability to integrate with State applications using, OpenID, OAuth, Web Services Federation Protocol (WS-Fed), Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), Active Directory, Application Programming Interface (API) or equivalent protocols.
P: Strong response

iv. ☒Ability to match the identity of the portal user to the identity of the same user in the Agency system.
P: Weak response (Covers Okta, but NOT Socure ID+)

v. ☒Log all actions taken by:
   i. Constituents
   ii. MaineIT Support, including:
      (a) Who made the change
      (b) When the change was made
      (c) What changed to and from
N: Weak response (Covers Okta, but NOT Salesforce, NOT Socure ID+)

vi. ☒Logging data must be available for system dashboards and reporting.
N: Weak response (Covers Okta, but NOT Salesforce, NOT Socure ID+)

d. Customer Service
The State is seeking solution(s) to provide 24/7/365 customer service to Constituents regardless of their location or technical abilities.
   i. ☒Support Constituents with personalized and timely assistance.
   ii. ☒Provide the state options to support our Constituents across multiple channels including, but not limited to phone, email, chat, etc.
P: Strong response
Q: Was it included in the Cost Proposal?

C.1. General System
   a. ☒Mobile support with native app (iOS and Android)
   b. ☒System availability: 24/7 with a maximum of four (4) 1-hour outages per

year

c. ☒Identity relationships must be tracked in the cloud infrastructure.
d. ☒Support responsive web and web browsers.
   i. ☒Supports Windows, Chrome, and Macintosh operating systems.

P: Strong responses

C.2. ☒Compliance with MaineIT Policies & Standards

a. Architecture Compliance Policy
b. System and Services Acquisition Policy and Procedures (SA-1)
c. Application Deployment Certification Policy
d. Digital Accessibility Policy
e. Remote Hosting Policy
f. Data Exchange Policy
g. Information Security Policy
h. Access Control Policy (AC-1)
i. Access Control Procedures for Users (AC-2)
j. Risk Assessment Policy and Procedures (RA-1)
k. Vulnerability Scanning Procedure (RA-5)
l. Security Assessment and Authorization Policy and Procedures (CA-1)
m. System and Information Integrity Policy and Procedures (SI-1)
n. Configuration Management Policy (CM-1)
o. Web Standards

P: Strong response

C.3. Support and Maintenance

a. ☒Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State’s official acceptance of the implemented solution.
   P: Strong response

b. ☒Terms and duration of the support and maintenance will be specified in the contract.
   P: Strong response

c. ☒All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
   P: Strong response

d. ☒Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
P: Strong response

e. ☒All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
P: Strong response

f. ☒All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
P: Adequate response

g. ☒User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
P: Adequate response

4. Security

The proposed solutions must provide a robust security system that aligns with the States Security Policies, standards, and Processes, Including:

Comply with or have the following security certifications:

i. ☒National Institute of Standards and Technology (NIST) 800-53
ii. ☒FedRamp
iii. ☒Health Insurance Portability and Accountability Act (HIPAA)
iv. ☒SOC 2 Type II
v. ☒Comply to the following security controls:
vi. ☒DDOS Protections [WN1]
vii. ☒Open Web Application Security Project (OWASP) Top 10
viii. ☒Cross Site Scripting
ix. ☒Structured Query Language (SQL) Injection
x. ☒Authentication bypass
xi. ☒Poorly authenticated APIs
xii. ☒Role based access controls
xiii. ☒Proper session control
xiv. ☒Real-time visibility

xv. ☒Anomalous behavior
xvi. ☒User sign with geo-location tracking
xvii. ☒Geo-blocking capabilities.
xviii. ☒Web Application Firewall [WN1]
xix. ☒System security must include the following security components:
xx. ☒Account take over protections
xxi. ☒Account sign-in Protections
xxii. ☒Behavior detection and evaluation
xxiii. ☒Adaptive AI Technology
xxiv. ☒Bot Protection; identity visitor behavior through analysis, technical and behavioral data.
xxv. ☒The proposed solution must be able to integrate with the State Security Information and Event Monitoring (SIEM) Splunk. Ability to log security information and events.

P: Strong response

5. Licensing

☒The State is aware that multiple licensing options are available and will be required to support the proposed solution in its entirety. The State seeks bids which will provide the most cost-effective licensing approach. Bidders are required to provide a detail breakdown for the proposed licensing.

Q: Strong response

1. Training and OCM (Organizational Change Management)

a. ☒Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
b. ☒Training must include technical and administrator training, initial and ongoing as users are added.
c. ☒Continuous process to ensure Constituents that may have run into issues setting up accounts have help 24/7.
d. ☒Bidders shall guide the State in OCM engagement for the duration of project planning, transition, and final implementation phase including:
    i. Designing and managing team structures with roles and responsibilities to facilitate automated program delivery, while noting any risks anticipated from the lack of readiness in the organization and staffing.
    ii. Ensure a successful transition for the integration of new processes and technology with stakeholders.

iii. Organizational readiness assessment

P: Strong response

3. **Disaster Recovery**
   a. ☒Availability of ninety-nine-point nine percent (99.9%) of uptime
   b. ☒Capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six (6) hours (i.e., maximum data loss cannot exceed six (6) hours)
   c. ☒Recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours.

   P: Adequate response

4. **Feature Enhancements**

a. ☒The State is seeking two hundred and fifty (250) hours of time and material for each proposed technology (CIAM), Personalized Dashboard, Disclosure and Consent Management, Data Management, and Recommendation Technology) to allow for specifications and enhancements during the contract period.

P: Adequate response

5. **Project Management**
   a. ☒The State plans to have its own project manager however, the awarded Bidder must have a project manager that has the primary responsibility for executing the project management tasks associated with the project. The awarded Bidder will:
      i. Work in collaboration with the State's Project Manager
      ii. Align with State Project Management processes and practices.
   b. ☒Manage the implementation, executing all activities, tasks, deliverables and resource needs, both state and awarded Bidder.
   c. ☒Track project status including managing and tracking all project risks, issues and decisions.
   d. ☒Track and report status of deliverables and project status
   e. ☒The awarded Bidder will provide their approach for project management and administration services including:
      i. Project Management Methodology
      ii. Project Governance
      iii. Resource Allocation and Schedule Management approach
      iv. Communication Management Approach including status reporting and document repository management.

v. Risk and Issue Management Methodology
vi. Change Management Methodology
vii. Quality Management Methodology

P: Strong response

D. Value Added Options (Other)

☒Bidders shall provide value added optional services to address relevant matters that have not been anticipated in this RFP but contribute to successful implementation of the proposed solutions, as well as any technology or services that will reduce risk to the project's quality and continuity. The value-added technology and services will not be included in the evaluation process but may be added during the contract negotiations.

P: Three elaborate options

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Deloitte
DATE: 5/29/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

Section I – Preliminary Information (No points – Eligibility Requirements)

(File #1 App. A, B, C)

☒Done – Pass/Fail by Procurement & RFP Coordinator

Section II Organization Qualifications and Experience

(File #2 – App. D, E + other areas that have no Appendix number but are part of File #2)

File 2 was not included in bidder submission.

1. **Overview of the Organization (App. D)**

   ☐Bidders must include three examples of projects which demonstrate their experience and expertise in performing these services as well as highlighting the Bidder's stated qualifications and skills.

   Statement of qualifications

   ☐Client name, contact person, Ph#, email.

   Contract history with the state may be considered in rating proposals even if not provided by the bidder.

   P, N, Q, or I & Notes:

2. **Subcontractors (App. E)**

   ☐If subcontractors are to be used, Bidders must provide the name, address, phone number, contact person, and a brief description of the subcontractors' organizational capacity and qualifications.

   Business name, contact person, address, ph#, email.

   P, N, Q, or I & Notes:

3. **Organizational Chart (No Appendix)**

   ☐Bidders must provide an organizational chart. The organizational chart must include the project being proposed. Each position must be identified by position title and corresponding to the personnel job descriptions.

   P, N, Q, or I & Notes:

4. **Litigation (No App.)**

☐Bidders must attach a list of all current litigation in which the Bidder is named and a list of all closed cases that have closed within the past five (5) years in which the Bidder paid the claimant either as part of a settlement or by decree. For each, list the entity bringing suit, the complaint, the accusation, amount, and outcome.
P, N, Q, or I & Notes:

5. **Financial Viability (No App.)**
☐Bidders must provide a current copy of their Dun & Bradstreet Business Information Report Snapshot.
P, N, Q, or I - Notes:

6. **Licensure/Certification (No App.)**
☐Bidders *may* provide documentation of any applicable licensure/certification or specific credentials that are related to providing the proposed services of the RFP.
P, N, Q, or I & Notes:

7. **Certificate of Insurance (No App.)**
☐Bidders must provide a certificate of insurance on a standard ACORD form (or the equivalent) evidencing the Bidder's general liability, professional liability and any other relevant liability insurance policies that might be associated with the proposed services.
P, N, Q, or I & Notes:
File 2 was not included in bidder submission.

Section III - Proposed Services

(File #3 – App. F, G, H)

1. **Technical Assessment (App. F)**
☒Done

2. **Services to be Provided (App. G)**

Note: on App. G Detailed Technical and Functional Requirements Excel spreadsheet, a tab is labeled User Stories. No response is required for Tab 3; these were provided to bidders for clarity and understanding of the expected journey a Constituent will experience.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Deloitte
DATE: 5/29/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes: P – addressed all areas thoroughly	**1. System security components System security must include the following security components:**
	1) Account Take Over Protections
	a) Account Sign-in Protections
	a) Account Sign-in Protections
	a) Adaptive AI Technology
	b) Bot Protection: identify visitor behavior through analysis of technical and behavioral data.
☐ P, Q, N or I Notes: : P – addressed all areas thoroughly. WOW: 2) Accessibility features for visually impaired users and support of WCAG 2.1 AA standards, including voice assistance	**2. Identity Proofing must have the ability to provide levels of proofing which will be directly tied to the constituent's level of access.**
	1) Define various levels of id proofing
	2) Document Image Capture
	3) Close coupling with authentication
☒ P, Q, N or I Notes: P	**3. Multi-factor authentication The system must support multi-factor authentication to protect against user impersonation and credential theft.**
☒ : P – listed many more factors than device/location.	**4. Risk-based factors The system must support risk-based factors and scores that are based on factors such as, but not limited to, device and location.**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Deloitte
DATE: 5/29/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

P, Q, N or I Notes:	
☒ P, Q, N or I Notes: P – addressed all areas thoroughly	**5. Identity lifecycle management components The system must include the following identity lifecycle management components for risk-based critical applications not limited to end users but also for generic accounts and system/service accounts:**
	1) Identity Creation
	2) Identity provisioning
	3) Attribute maps
	4) Authentication (e.g., password policies and synchronization)

☒ P, Q, N or I Notes: Q – did not mention Azure, Oracle, Google,	**6. Security event logging The system must log security information and events.**
	Security Information and Event Management (SIEM) – Splunk
	Cloud Services: Azure, AWS, Oracle, Google
☒ P, Q, N or I Notes: P – addressed all areas thoroughly	**7. Security Certifications The system must comply too or have the following security certifications:**

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Deloitte
DATE: 5/29/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

	1) NIST 800-53
	2) FedRamp
	3) HIPAA
	4) SOC 2 Type II
	Note:
	IRS require a 45-day letter approval for new cloud solutions.
☒ P, Q, N or I Notes: P – addressed all areas thoroughly	**8. SIEM (Splunk) integration The system must be able to integrate with the State of Maine Security Information and Event Monitoring (SIEM) Splunk for Security Operations Center operations.**
☒ P, Q, N or I Notes: P – addressed all areas thoroughly	**9. Core constituent data. The system must maintain a central repository of basic (core) constituent data, that can be used by any SoM application to reduce data redundancy and outdated or inaccurate information while maintaining confidentiality.**
☒ P, Q, N or I Notes: P – addressed all areas thoroughly	**11. Data Management. The system must apply the Data Management Rules to the constituent profile data as per the SoM Data Management Policies.**
☒ P, Q, N or I Notes: P – addressed all areas thoroughly	**12. SOM Employee. The system must support multiple identities for SOM employees that work with the portal in a support role.**
	1) SOM Employee identity and credentials for supporting the application.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Deloitte
DATE: 5/29/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

	2) Constituent identity and credentials to use the state services offered through the portal.

☒ P, Q, N or I Notes: P – addressed all areas thoroughly	**13. APIs. The system must be able to connect to at least one agency application.**
	Considerations:
	a) OpenID, OAuth, WS-Fed, SAML, LDAP, Active Directory, Application Programming Interfaces (APIs), Software Development
	b) Develop once and reuse often with other agencies would be ideal
☒ P, Q, N or I Notes: P – addressed all areas thoroughly	**14. User identification matching. The system must be able to match the identity of the portal user to the identity of the same user in the agency system.**
☒ P, Q, N or I Notes: P – addressed all areas thoroughly	**15. Single sign-on. The system must support single sign-on to the agency application.**
☒ P, Q, N or I Notes: P – addressed all areas thoroughly	**16. Import user profile data from agency systems. The system must be able to import user data from different SoM applications to ensure offboarding happens in a timely manner, so that government resources are protected from fraud. (example: death records)**
☒ P, Q, N or I Notes: P – addressed	**17. History logging.** 1) The system must log all actions taken by:

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Deloitte
DATE: 5/29/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

all areas thoroughly	
	a) Constituents
	b) MaineIT support
	Including but not limited to:
	c) who made the change
	d) when the change was made
	e) what changed
☒ P, Q, N or I Notes: P – addressed all areas thoroughly	**18. Reporting. The logging data (history) must be available for constituent and system dashboards and reporting in general.**
☒ P, Q, N or I Notes: P – addressed all areas thoroughly	**19. Security Controls. The system must comply to the following security controls:**
	1) DDOS Protections[WN1] ,
	2) OWASP Top 10
	a) Cross Site Scripting,
	b) SQL Injection,
	3) Authentication bypass,
	a) poorly authenticated APIs,
	b) Role based access controls,
	c) proper session control
	4) Real-time visibility,
	5) Anomalous behavior,
	6) User sign with geo-location tracking,
	Geo-blocking capabilities.
	Security controls must include Web Application Firewall [WN1]
☒	**20. General System Requirements.**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Deloitte
DATE: 5/29/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

P, Q, N or I Notes: P – addressed all areas thoroughly – very nice: Prioritizing wireframing, prototyping, and usability testing for mobile devices	1) Mobile Support with Native App; (iOS and Android)
	2) System availability: 24/7 with 4x1-hour outages per year
	3) Identity relationships must be tracked in the cloud infrastructure.
	4) Support responsive web and web browsers.
	a. Supports Windows, Chrome, and Macintosh operating systems
☒ P, Q, N or I Notes: P – We did not specify in this area that the 24/7 was via phone so this bidder did respond well	**21. Training and Support.** 1) Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
	2) MaineIT will require technical/administrator training. There will be initial training and on-going training as users are added.
	3) Have a continuous process to ensure constituents that may have run into issues setting up accounts can have help 24/7.
☒	**22. Support Requirements**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Deloitte
DATE: 5/29/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

P, Q, N or I Notes: : P – addressed all areas thoroughly	1) The Bidder will provide support, and maintenance for the solution to begin immediately after receiving the State's official acceptance of the implemented solution.
	2) Support and maintenance will be provided for the terms and duration specified in the contract.
	3) The Bidder will address all questions and reported problems related to the technical and functional operation of the system.
	4) The Bidder must provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours: 8:00 a.m. to 5:00 p.m. Eastern Standard Time.
	5) As part of the maintenance agreement, the Bidder will make all product releases and upgrades available to the State at no additional charge.
	6) All release and upgrades shall be implemented and tested by the Bidder, outside of the normal operating hours of the State government.
	7) User testing shall occur during normal State business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State government.
☒ P, Q, N or I Notes: : P – addressed all areas thoroughly	**23. Hosting** Solution can comply with MaineIT remote hosting policies. a) Remote Hosting Policy http://maine.gov/oit/policies/RemoteHostingPolicy.pdf b) Hosting Customization Policy http://maine.gov/oit/policies/HostingCustomizationPolicy.pdf
☒ P, Q, N or I Notes: : P – addressed all areas thoroughly – 4,5,6 Deloitte states they	**24. Disaster Recovery** Proposed Solution can comply with MaineIT security requirements and remote hosting requirements, without requiring waivers, before contract finalization.

will facilitate this on our behalf	
	1) Maintaining an availability metric of ninety-nine-point nine percent (99.9%) of uptime
	2) Ensuring the capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six hours (i.e., maximum data loss cannot exceed six (6) hours);
	3) Ensuring a recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours;
	4) Ensuring the hosting environment provides adequate capacity to ensure that, under ethernet connectivity to the client device, data inquiry/lookup response is within three (3) seconds, and data modification response is within five (5) seconds;
	5) Providing the Department at least thirty (30) calendar day advance written notice of any material change in network operations or architecture;
	6) Ensuring any planned material change in network operations or architecture cannot be made without the prior written consent of the Department; and Outlining of all Service Level Agreements (SLAs) for technical support (the awarded Bidder shall be open to negotiation to ensure the SLAs meet the Department's needs

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

☒1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
P, N, Q, or I & Notes: Q – pg. 5 of App. H states that the dashboard is FedRAMP moderate, is that good enough? Pg. 9 – great scenarios presented. Pg. 10 – good focus on accessibility and usability testing. Pg. 15 – great architecture graphic

☐1b) Detailed description of the technologies, software and / or hardware for each of the components.

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Deloitte
DATE: 5/29/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

P, N, Q, or I & Notes:

☒1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.
P, N, Q, or I & Notes: P

☒1d) Description of the overall platform and architecture of the proposed solution(s).
P, N, Q, or I & Notes: P

☒1e) Description of any third-party software or partnerships required for the proposed Solution(s).
P, N, Q, or I & Notes: P

☒2a) A detailed timeline and description of milestones, deliverables, tasks
P, N, Q, or I & Notes: P – pg. 18 – 20, well done.

☒2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period
P, N, Q, or I & Notes: P pt. 21

☒2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
P, N, Q, or I & Notes: P

☒2d) Average time to market for each component.
P, N, Q, or I & Notes: P

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. ☒Capture Constituent Identity and profile data. Pg. 37
   P, N, Q, or I & Notes: P
b. ☒Provide identity provisioning and deprovisioning.
   P, N, Q, or I & Notes: P
c. ☒Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
   i. Identity Creation
   ii. Identity provisioning
   iii. Attribute maps
   iv. Authentication (e.g., password policies and synchronization)
      P, N, Q, or I & Notes: P
d. ☒Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies.
   P, N, Q, or I & Notes: P
e. ☒Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
   P, N, Q, or I & Notes: P pg. 40 - 41, thorough description.
f. ☐Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.
   P, N, Q, or I & Notes: P Pg. 42
g. ☒Allow for multiple role selections for the following identities:
   i. Individual
   ii. Business Owner
   iii. Support multiple identities for State employees that work with the portal in a support role:
      (a) SOM Employee identity and credentials for supporting the application.
      (b) Constituent identity and credentials to use the state services offered through the portal.
   iv. Multi role individual (Individual and Business Owner)
      P, N, Q, or I & Notes: P

h. ☒Have the ability to provide levels of proofing which will be directly tied to the Constituent's level of consent given.
P, N, Q, or I & Notes: P

i. ☒Support multi-factor authentication to protect against user impersonation and credential theft.
P, N, Q, or I & Notes: P

B.2. ☒The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.
P, N, Q, or I & Notes:

a. Disclosure and Consent Management

The desire of the State is to be as transparent as possible and respect the privacy of the individual interacting with the Constituents' Portal. Consent is a core tenant of maintaining the public trust in the Constituents' Portal and will be a foundational component of the architecture.

The Disclosure and Consent Management solution shall include:

i. ☒Granular consent management that encompasses the automated functions necessary to create, modify, revoke, and manage Constituent consents.
ii. ☒Allow users the ability to opt-in and opt-out of data sharing and services within the Constituents' portal. Pg. 51, good representation.
iii. ☒Obtain user consent both in an interactive and set preference mode for a variety of transactions on the Portal.
iv. ☒Support administrative users' management of standard legal disclaimers and data classification for transactions.
v. ☒Highly configurable with version control and history tracking for consent language.

vi. ☒Ability for end user to access a retrievable log of granted consent and data usage on the portal derived from the consent.

P, N, Q, or I & Notes: P – VERY well done!

b. Recommendation Technology

The State is seeking options which, while maintaining individual privacy, will collect and analyze data about user interactions, behavior, and preferences. The expected outcome of this will be to provide insights and intelligence that help the State make informed decisions and improve Constituent experiences.

i. ☒From the user perspective, the portal should be able to make real-time recommendations for related services.
ii. ☐Data captured in this environment must be obfuscated, as to not allow any party to directly target or track the preferences of an individual or their usage of the portal.
iii. ☐Solution providers should discuss in detail their use, storage, destruction of metadata, and tracking technologies with emphasis on how their offering provides analytical insights while protecting the individual user privacy.

P, N, Q, or I & Notes: Q – I did not see ii. And iii. Addressed in the pages 50-55

c. Data Management

The State is seeking the ability for the portal’s Constituent identity to be linked to records maintained by individual State agencies. The proposed solution will include:

i. ☒Capabilities to streamline the sharing of data between State systems, including
    i. The identity assurance level
    ii. Agency to user notifications
    iii. Verification of user consent
    iv. Identity resolution
    v. Data sharing between agencies.
ii. ☒Maintain a central repository of basic (core) Constituent data, that can be used by any State application to reduce data redundancy, and outdated or inaccurate information while maintaining confidentiality.
iii. ☒Ability to integrate with State applications using, OpenID, OAuth, Web Services Federation Protocol (WS-Fed), Security Assertion Markup

Language (SAML), Lightweight Directory Access Protocol (LDAP), Active Directory, Application Programming Interface (API) or equivalent protocols.

- iv. ☒Ability to match the identity of the portal user to the identity of the same user in the Agency system.
- v. ☒Log all actions taken by:
  - i. Constituents
  - ii. MaineIT Support, including:
    - (a) Who made the change
    - (b) When the change was made
    - (c) What changed to and from
- vi. ☒Logging data must be available for system dashboards and reporting.

P, N, Q, or I & Notes: P

d. Customer Service

The State is seeking solution(s) to provide 24/7/365 customer service to Constituents regardless of their location or technical abilities.

- i. ☒Support Constituents with personalized and timely assistance.
- ii. ☒Provide the state options to support our Constituents across multiple channels including, but not limited to phone, email, chat, etc.

P, N, Q, or I & Notes: P – currently support 20 states with contact centers.

C.1. General System

- a. ☒Mobile support with native app (iOS and Android)
- b. ☒System availability: 24/7 with a maximum of four (4) 1-hour outages per year
- c. ☒Identity relationships must be tracked in the cloud infrastructure.
- d. ☒Support responsive web and web browsers.
  - i. ☒Supports Windows, Chrome, and Macintosh operating systems.

P, N, Q, or I & Notes: P

C.2. ☐Compliance with MaineIT Policies & Standards

- a. Architecture Compliance Policy
- b. System and Services Acquisition Policy and Procedures (SA-1)
- c. Application Deployment Certification Policy
- d. Digital Accessibility Policy

e. Remote Hosting Policy
f. Data Exchange Policy
g. Information Security Policy
h. Access Control Policy (AC-1)
i. Access Control Procedures for Users (AC-2)
j. Risk Assessment Policy and Procedures (RA-1)
k. Vulnerability Scanning Procedure (RA-5)
l. Security Assessment and Authorization Policy and Procedures (CA-1)
m. System and Information Integrity Policy and Procedures (SI-1)
n. Configuration Management Policy (CM-1)
o. Web Standards

P, N, Q, or I & Notes: P – very well done. Pg. 65

C.3. Support and Maintenance

a. ☒Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State's official acceptance of the implemented solution.
P, N, Q, or I & Notes:

b. ☒Terms and duration of the support and maintenance will be specified in the contract.
P, N, Q, or I & Notes:

c. ☒All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
P, N, Q, or I & Notes:

d. ☒Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
P, N, Q, or I & Notes:

e. ☒All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
P, N, Q, or I & Notes:

f. ☒All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
P, N, Q, or I & Notes:

g. ☒User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
P, N, Q, or I & Notes: P

4. Security

The proposed solutions must provide a robust security system that aligns with the States Security Policies, standards, and Processes, Including:

Comply with or have the following security certifications:

i. ☒National Institute of Standards and Technology (NIST) 800-53
ii. ☒FedRamp
iii. ☒Health Insurance Portability and Accountability Act (HIPAA)
iv. ☒SOC 2 Type II
v. ☐Comply to the following security controls:
vi. ☒DDOS Protections [WN1]
vii. ☒Open Web Application Security Project (OWASP) Top 10
viii. ☒Cross Site Scripting
ix. ☒Structured Query Language (SQL) Injection
x. ☒Authentication bypass
xi. ☒Poorly authenticated APIs
xii. ☒Role based access controls
xiii. ☒Proper session control
xiv. ☐Real-time visibility
xv. ☐Anomalous behavior
xvi. ☐User sign with geo-location tracking
xvii. ☐Geo-blocking capabilities.
xviii. ☐Web Application Firewall [WN1]
xix. ☐System security must include the following security components:
xx. ☐Account take over protections
xxi. ☐Account sign-in Protections
xxii. ☐Behavior detection and evaluation
xxiii. ☐Adaptive AI Technology
xxiv. ☐Bot Protection; identity visitor behavior through analysis, technical and behavioral data.

xxv. ☒The proposed solution must be able to integrate with the State Security Information and Event Monitoring (SIEM) Splunk. Ability to log security information and events.

P, N, Q, or I & Notes: P

5. Licensing

☒The State is aware that multiple licensing options are available and will be required to support the proposed solution in its entirety. The State seeks bids which will provide the most cost-effective licensing approach. Bidders are required to provide a detail breakdown for the proposed licensing.

P, N, Q, or I & Notes: P – very detailed, pg. 80

1. Training and OCM (Organizational Change Management)

a. ☒Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
b. ☒Training must include technical and administrator training, initial and ongoing as users are added.
c. ☒Continuous process to ensure Constituents that may have run into issues setting up accounts have help 24/7.
d. ☒Bidders shall guide the State in OCM engagement for the duration of project planning, transition, and final implementation phase including:
    i. Designing and managing team structures with roles and responsibilities to facilitate automated program delivery, while noting any risks anticipated from the lack of readiness in the organization and staffing.
    ii. Ensure a successful transition for the integration of new processes and technology with stakeholders.
    iii. Organizational readiness assessment

P, N, Q, or I & Notes: P

3. Disaster Recovery

a. ☒Availability of ninety-nine-point nine percent (99.9%) of uptime
b. ☐Capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six (6) hours (i.e., maximum data loss cannot exceed six (6) hours)

c. ☐Recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours.

P, N, Q, or I & Notes: N – did not address 6 hour time frame or 2 hour RTO.

4. Feature Enhancements

a. ☒The State is seeking two hundred and fifty (250) hours of time and material for each proposed technology (CIAM), Personalized Dashboard, Disclosure and Consent Management, Data Management, and Recommendation Technology) to allow for specifications and enhancements during the contract period.

P, N, Q, or I & Notes: P

5. Project Management

a. ☒The State plans to have its own project manager however, the awarded Bidder must have a project manager that has the primary responsibility for executing the project management tasks associated with the project. The awarded Bidder will:
    i. Work in collaboration with the State's Project Manager
    ii. Align with State Project Management processes and practices.
b. ☒Manage the implementation, executing all activities, tasks, deliverables and resource needs, both state and awarded Bidder.
c. ☒Track project status including managing and tracking all project risks, issues and decisions.
d. ☒Track and report status of deliverables and project status
e. ☒The awarded Bidder will provide their approach for project management and administration services including:
    i. Project Management Methodology
    ii. Project Governance
    iii. Resource Allocation and Schedule Management approach
    iv. Communication Management Approach including status reporting and document repository management.
    v. Risk and Issue Management Methodology
    vi. Change Management Methodology
    vii. Quality Management Methodology

P, N, Q, or I & Notes:

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Deloitte
DATE: 5/29/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

D. Value Added Options (Other)

☒Bidders shall provide value added optional services to address relevant matters that have not been anticipated in this RFP but contribute to successful implementation of the proposed solutions, as well as any technology or services that will reduce risk to the project's quality and continuity. The value-added technology and services will not be included in the evaluation process but may be added during the contract negotiations.

P, N, Q, or I & Notes: P – some very nice ideas, most especially the SOS part.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Microsoft
DATE: 6/6/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

Section I – Preliminary Information (No points – Eligibility Requirements)

(File #1 App. A, B, C)

☒Done – Pass/Fail by Procurement & RFP Coordinator

Section II Organization Qualifications and Experience

(File #2 – App. D, E + other areas that have no Appendix number but are part of File #2)

1. Overview of the Organization (App. D)

☒Bidders must include three examples of projects which demonstrate their experience and expertise in performing these services as well as highlighting the Bidder's stated qualifications and skills.

Statement of qualifications

☐Client name, contact person, Ph#, email.

Contract history with the state may be considered in rating proposals even if not provided by the bidder.

P, **N**, Q, or I & Notes:

Missing contact information

2. Subcontractors (App. E)

☒If subcontractors are to be used, Bidders must provide the name, address, phone number, contact person, and a brief description of the subcontractors' organizational capacity and qualifications.

Business name, contact person, address, ph#, email.

P, N, Q, or I & Notes:

3. Organizational Chart (No Appendix)

☒Bidders must provide an organizational chart. The organizational chart must include the project being proposed. Each position must be identified by position title and corresponding to the personnel job descriptions.

P, N, Q, or I & Notes:

4. Litigation (No App.)

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Microsoft
DATE: 6/6/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

☐Bidders must attach a list of all current litigation in which the Bidder is named and a list of all closed cases that have closed within the past five (5) years in which the Bidder paid the claimant either as part of a settlement or by decree. For each, list the entity bringing suit, the complaint, the accusation, amount, and outcome.
P, **N**, Q, or **I** & Notes:
Document not provided

5. **Financial Viability (No App.)**
☐Bidders must provide a current copy of their Dun & Bradstreet Business Information Report Snapshot.
P, **N**, Q, or I - Notes:
Dun & Bradstreet documentation not provided

6. **Licensure/Certification (No App.)**
☒Bidders *may* provide documentation of any applicable licensure/certification or specific credentials that are related to providing the proposed services of the RFP.
P, N, Q, or **I** & Notes:

7. **Certificate of Insurance (No App.)**
☐Bidders must provide a certificate of insurance on a standard ACORD form (or the equivalent) evidencing the Bidder's general liability, professional liability and any other relevant liability insurance policies that might be associated with the proposed services.
P, **N**, Q, or **I** & Notes:
Document not provided

Section III - Proposed Services

(File #3 – App. F, G, H)

1. **Technical Assessment (App. F)**
☒Done

2. **Services to be Provided (App. G)**

Note: on App. G Detailed Technical and Functional Requirements Excel spreadsheet, a tab is labeled User Stories. No response is required for Tab 3; these were provided to bidders for clarity and understanding of the expected journey a Constituent will experience.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Microsoft
DATE: 6/6/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, **N** or I Notes: Other than listing which technology – no explanation of how technology/protections work	**1. System security components System security must include the following security components:**
	1) Account Take Over Protections
	a) Account Sign-in Protections
	a) Account Sign-in Protections
	a) Adaptive AI Technology
	b) Bot Protection: identify visitor behavior through analysis of technical and behavioral data.
☒ P, Q, **N** or I Notes: no definition for any or explanation proofing	**2. Identity Proofing must have the ability to provide levels of proofing which will be directly tied to the constituent's level of access.**
	1) Define various levels of id proofing
	2) Document Image Capture
	3) Close coupling with authentication
☒ P, Q, N or **I** Notes: no real definition	**3. Multi-factor authentication The system must support multi-factor authentication to protect against user impersonation and credential theft.**
☒ P, Q, **N** or I Notes: no explanation other than provided by Socure; no detail on how	**4. Risk-based factors The system must support risk-based factors and scores that are based on factors such as, but not limited to, device and location.**
☒ P, Q, **N** or I Notes: no explanation other than provided by Azure B2C; no detail	**5. Identity lifecycle management components The system must include the following identity lifecycle management components for risk-based critical applications not limited to end users but also for generic accounts and system/service accounts:**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Microsoft
DATE: 6/6/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

	1) Identity Creation
	2) Identity provisioning
	3) Attribute maps
	4) Authentication (e.g., password policies and synchronization)

☒ P, Q, N or **I** Notes:	**6. Security event logging The system must log security information and events.**
	Security Information and Event Management (SIEM) – Splunk
	Cloud Services: **Azure**, AWS, Oracle, Google
☒ P, Q, N or **I** Notes:	**7. Security Certifications The system must comply too or have the following security certifications:**
	1) NIST 800-53
	2) FedRamp
	3) HIPAA
	4) SOC 2 Type II
	Note:
	IRS require a 45-day letter approval for new cloud solutions.
☒ P, Q, N or **I** Notes:	**8. SIEM (Splunk) integration The system must be able to integrate with the State of Maine Security Information and Event Monitoring (SIEM) Splunk for Security Operations Center operations.**
☒ P, Q, **N** or I	**9. Core constituent data. The system must maintain a central repository of basic (core) constituent data, that can be used by any SoM application to reduce data redundancy**

Notes: no mention of a repository	**and outdated or inaccurate information while maintaining confidentiality.**
☒ P, Q, **N** or I Notes: no details provided	**11. Data Management. The system must apply the Data Management Rules to the constituent profile data as per the SoM Data Management Policies.**
☒ P, Q, N or **I** Notes:	**12. SOM Employee. The system must support multiple identities for SOM employees that work with the portal in a support role.**
	1) SOM Employee identity and credentials for supporting the application.
	2) Constituent identity and credentials to use the state services offered through the portal.

☒ P, Q, N or **I** Notes:	**13. APIs. The system must be able to connect to at least one agency application.**
	Considerations:
	a) OpenID, OAuth, WS-Fed, SAML, LDAP, Active Directory, Application Programming Interfaces (APIs), Software Development
	b) Develop once and reuse often with other agencies would be ideal
☒ P, Q, **N** or i Notes: not enough details around how	**14. User identification matching. The system must be able to match the identity of the portal user to the identity of the same user in the agency system.**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Microsoft
DATE: 6/6/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or **I** Notes:	**15. Single sign-on. The system must support single sign-on to the agency application.**
☒ P, Q, **N** or I Notes: Lacking detail	**16. Import user profile data from agency systems. The system must be able to import user data from different SoM applications to ensure offboarding happens in a timely manner, so that government resources are protected from fraud. (example: death records)**
☒ P, Q, N or **I** Notes:	**17. History logging.** 1) The system must log all actions taken by:
	a) Constituents
	b) MaineIT support
	Including but not limited to:
	c) who made the change
	d) when the change was made
	e) what changed
☒ P, Q, N or **I** Notes:	**18. Reporting. The logging data (history) must be available for constituent and system dashboards and reporting in general.**
☒ P, Q, N or **I** Notes:	**19. Security Controls. The system must comply to the following security controls:**
	1) DDOS Protections[WN1] ,
	2) OWASP Top 10
	a) Cross Site Scripting,
	b) SQL Injection,
	3) Authentication bypass,
	a) poorly authenticated APIs,
	b) Role based access controls,
	c) proper session control

	4) Real-time visibility,
	5) Anomalous behavior,
	6) User sign with geo-location tracking,
	Geo-blocking capabilities.
	Security controls must include Web Application Firewall [WN1]
☒ P, Q, N or **I** Notes:	**20. General System Requirements.** 1) Mobile Support with Native App; (iOS and Android)
	2) System availability: 24/7 with 4x1-hour outages per year
	3) Identity relationships must be tracked in the cloud infrastructure.
	4) Support responsive web and web browsers.
	a. Supports Windows, Chrome, and Macintosh operating systems
☒ P, Q, **N** or I Notes:	**21. Training and Support.** 1) Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
No proposed plan	2) MaineIT will require technical/administrator training. There will be initial training and on-going training as users are added.
	3) Have a continuous process to ensure constituents that may have run into issues setting up accounts can have help 24/7.
☒ P, Q, **N** or I Notes:	**22. Support Requirements** 1) The Bidder will provide support, and maintenance for the solution to begin immediately after receiving the State's official acceptance of the implemented solution.
No proposed plan	2) Support and maintenance will be provided for the terms and duration specified in the contract.
	3) The Bidder will address all questions and reported problems related to the technical and functional operation of the system.
	4) The Bidder must provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented

	solution during regular business hours: 8:00 a.m. to 5:00 p.m. Eastern Standard Time.
	5) As part of the maintenance agreement, the Bidder will make all product releases and upgrades available to the State at no additional charge.
	6) All release and upgrades shall be implemented and tested by the Bidder, outside of the normal operating hours of the State government.
	7) User testing shall occur during normal State business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State government.
☒ P, Q, N or **I** Notes:	**23. Hosting** Solution can comply with MaineIT remote hosting policies. a) Remote Hosting Policy http://maine.gov/oit/policies/RemoteHostingPolicy.pdf b) Hosting Customization Policy http://maine.gov/oit/policies/HostingCustomizationPolicy.pdf
☒ P, Q, N or **I** Notes:	**24. Disaster Recovery** Proposed Solution can comply with MaineIT security requirements and remote hosting requirements, without requiring waivers, before contract finalization.
	1) Maintaining an availability metric of ninety-nine-point nine percent (99.9%) of uptime
	2) Ensuring the capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six hours (i.e., maximum data loss cannot exceed six (6) hours);
	3) Ensuring a recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours;
	4) Ensuring the hosting environment provides adequate capacity to ensure that, under ethernet connectivity to the client device, data inquiry/lookup response is within three (3) seconds, and data modification response is within five (5) seconds;
	5) Providing the Department at least thirty (30) calendar day advance written notice of any material change in network operations or architecture;
	6) Ensuring any planned material change in network operations or architecture cannot be made without the prior written consent of the Department; and Outlining of all Service Level Agreements

		(SLAs) for technical support (the awarded Bidder shall be open to negotiation to ensure the SLAs meet the Department's needs

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

☒1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
P, **N**, Q, or I & Notes:
Doesn't provide a complete description of solution; does not describe what partners are doing (whoami, socure, etc)

☒1b) Detailed description of the technologies, software and / or hardware for each of the components.
P, **N**, Q, or I & Notes:
Does not talk to consent, recommendations, etc

☒1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.
P, **N**, Q, or I & Notes:
Talks to methodology and frameworks, but not the solution

☒1d) Description of the overall platform and architecture of the proposed solution(s).
P, N, Q, or **I** & Notes: i like the break out of application and technical architecture

☒1e) Description of any third-party software or partnerships required for the proposed Solution(s).
P, **N**, Q, or I & Notes:
What about new era tech?

☒2a) A detailed timeline and description of milestones, deliverables, tasks
P, N, Q, or **I** & Notes:

☒2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through

Implementation Period and Post Implementation – Support period
P, N, Q, or I & Notes:

☒2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
P, N, Q, or **I** & Notes:

☒2d) Average time to market for each component.
P, N, Q, or **I** & Notes:

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. ☒Capture Constituent Identity and profile data.
   P, N, Q, or **I** & Notes:
b. ☒Provide identity provisioning and deprovisioning.
   P, N, Q, or **I** & Notes:
c. ☒Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
   i. Identity Creation
   ii. Identity provisioning
   iii. Attribute maps
   iv. Authentication (e.g., password policies and synchronization)
      P, N, Q, or **I** & Notes:
d. ☒Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies.
   P, **N**, Q, or I & Notes: does not talk to integration points
e. ☒Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
   P, N, Q, or **I** & Notes:
f. ☒Describe the extensibility of architecture so that future means of identity-

proofing (e.g. biometrics) may be incorporated.
P, N, Q, or **I** & Notes:

g. ☐Allow for multiple role selections for the following identities:
   i. Individual
   ii. Business Owner
   iii. Support multiple identities for State employees that work with the portal in a support role:
      (a) SOM Employee identity and credentials for supporting the application.
      (b) Constituent identity and credentials to use the state services offered through the portal.
   iv. Multi role individual (Individual and Business Owner)
   P, **N**, Q, or I & Notes: does not talk to any of the different personas

h. ☐Have the ability to provide levels of proofing which will be directly tied to the Constituent's level of consent given.
P, **N**, Q, or I & Notes: does not talk to consent

i. ☒Support multi-factor authentication to protect against user impersonation and credential theft.
P, N, Q, or **I** & Notes: mentioned as part of conditional access

B.2. ☒The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.
P, N, Q, or **I** & Notes:
Not a lot of detail on the how; however the mock ups talk to the requirement

a. Disclosure and Consent Management

The desire of the State is to be as transparent as possible and respect the privacy of the individual interacting with the Constituents' Portal. Consent is a core tenant of maintaining the public trust in the Constituents' Portal and will be a foundational component of the architecture.

The Disclosure and Consent Management solution shall include:

i. ☒Granular consent management that encompasses the automated functions necessary to create, modify, revoke, and manage Constituent consents.
ii. ☒Allow users the ability to opt-in and opt-out of data sharing and services within the Constituents' portal.
iii. ☐Obtain user consent both in an interactive and set preference mode for a variety of transactions on the Portal.
iv. ☐Support administrative users' management of standard legal disclaimers and data classification for transactions.
v. ☐Highly configurable with version control and history tracking for consent language.
vi. ☐Ability for end user to access a retrievable log of granted consent and data usage on the portal derived from the consent.

P, **N**, Q, or I & Notes:
Does not mention presetting a default consent; or if the logs are available back to the constituent

b. Recommendation Technology

The State is seeking options which, while maintaining individual privacy, will collect and analyze data about user interactions, behavior, and preferences. The expected outcome of this will be to provide insights and intelligence that help the State make informed decisions and improve Constituent experiences.

i. ☐From the user perspective, the portal should be able to make real-time recommendations for related services.
ii. ☐Data captured in this environment must be obfuscated, as to not allow any party to directly target or track the preferences of an individual or their usage of the portal.
iii. ☐Solution providers should discuss in detail their use, storage, destruction of metadata, and tracking technologies with emphasis on how their offering provides analytical insights while protecting the individual user privacy.

P, **N**, Q, or I & Notes:
Does not cover any of the above requirements

c. Data Management

The State is seeking the ability for the portal's Constituent identity to be linked to records maintained by individual State agencies. The proposed solution will include:

i. ☐Capabilities to streamline the sharing of data between State systems, including
  i. The identity assurance level
  ii. Agency to user notifications
  iii. Verification of user consent
  iv. Identity resolution
  v. Data sharing between agencies.
ii. ☐Maintain a central repository of basic (core) Constituent data, that can be used by any State application to reduce data redundancy, and outdated or inaccurate information while maintaining confidentiality.
iii. ☒Ability to integrate with State applications using, OpenID, OAuth, Web Services Federation Protocol (WS-Fed), Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), Active Directory, Application Programming Interface (API) or equivalent protocols.
iv. ☐Ability to match the identity of the portal user to the identity of the same user in the Agency system.
v. ☒Log all actions taken by:
  i. Constituents
  ii. MaineIT Support, including:
    (a) Who made the change
    (b) When the change was made
    (c) What changed to and from
vi. ☐Logging data must be available for system dashboards and reporting.

P, **N**, Q, or I & Notes:
Lacking detail for identification assurance

d. Customer Service

The State is seeking solution(s) to provide 24/7/365 customer service to Constituents regardless of their location or technical abilities.

i. ☒Support Constituents with personalized and timely assistance.
ii. ☐Provide the state options to support our Constituents across multiple channels including, but not limited to phone, email, chat, etc.

P, **N**, Q, or I & Notes:
Virtual/non human support model only

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Microsoft
DATE: 6/6/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

C.1. General System

a. ☒Mobile support with native app (iOS and Android)
b. ☒System availability: 24/7 with a maximum of four (4) 1-hour outages per year
c. ☒Identity relationships must be tracked in the cloud infrastructure.
d. ☒Support responsive web and web browsers.
    i. ☒Supports Windows, Chrome, and Macintosh operating systems.

P, N, Q, or **I** & Notes:

C.2. ☒Compliance with MaineIT Policies & Standards

a. Architecture Compliance Policy
b. System and Services Acquisition Policy and Procedures (SA-1)
c. Application Deployment Certification Policy
d. Digital Accessibility Policy
e. Remote Hosting Policy
f. Data Exchange Policy
g. Information Security Policy
h. Access Control Policy (AC-1)
i. Access Control Procedures for Users (AC-2)
j. Risk Assessment Policy and Procedures (RA-1)
k. Vulnerability Scanning Procedure (RA-5)
l. Security Assessment and Authorization Policy and Procedures (CA-1)
m. System and Information Integrity Policy and Procedures (SI-1)
n. Configuration Management Policy (CM-1)
o. Web Standards

P, N, Q, or **I** & Notes:

C.3. Support and Maintenance

a. ☒Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State’s official acceptance of the implemented solution.
   P, **N**, Q, or I & Notes:
   While they are recommending a support method it includes a technical contract utilized today for internal use. No tier 1 support
b. ☒Terms and duration of the support and maintenance will be specified in the contract.

P, N, Q, or **I** & Notes:

c. ☒All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
P, N, Q, or **I** & Notes:

d. ☐Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
P, **N**, Q, or I & Notes: not provided

e. ☒All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
P, N, Q, or **I** & Notes:

f. ☒All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
P, N, Q, or **I** & Notes:

g. ☒User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
P, N, Q, or **I** & Notes:

4. Security

The proposed solutions must provide a robust security system that aligns with the States Security Policies, standards, and Processes, Including:

Comply with or have the following security certifications:

i. ☒National Institute of Standards and Technology (NIST) 800-53
ii. ☒FedRamp
iii. ☒Health Insurance Portability and Accountability Act (HIPAA)
iv. ☒SOC 2 Type II
v. ☐Comply to the following security controls:
vi. ☒DDOS Protections [WN1]
vii. ☒Open Web Application Security Project (OWASP) Top 10
viii. ☐Cross Site Scripting
ix. ☐Structured Query Language (SQL) Injection
x. ☐Authentication bypass
xi. ☒Poorly authenticated APIs

xii. ☐Role based access controls
xiii. ☐Proper session control
xiv. ☐Real-time visibility
xv. ☐Anomalous behavior
xvi. ☐User sign with geo-location tracking
xvii. ☐Geo-blocking capabilities.
xviii. ☐Web Application Firewall [WN1]
xix. ☐System security must include the following security components:
xx. ☐Account take over protections
xxi. ☐Account sign-in Protections
xxii. ☐Behavior detection and evaluation
xxiii. ☐Adaptive AI Technology
xxiv. ☐Bot Protection; identity visitor behavior through analysis, technical and behavioral data.
xxv. ☒The proposed solution must be able to integrate with the State Security Information and Event Monitoring (SIEM) Splunk. Ability to log security information and events.

P, **N**, Q, or **I** & Notes:

Does not provide detail to unchecked boxes above

5. Licensing

☒The State is aware that multiple licensing options are available and will be required to support the proposed solution in its entirety. The State seeks bids which will provide the most cost-effective licensing approach. Bidders are required to provide a detail breakdown for the proposed licensing.

P, **N**, Q, or **I** & Notes:

Does not provide what is currently under our existing EA

1. Training and OCM (Organizational Change Management)

a. ☒Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
b. ☒Training must include technical and administrator training, initial and ongoing as users are added.
c. ☐Continuous process to ensure Constituents that may have run into issues setting up accounts have help 24/7.
d. ☒Bidders shall guide the State in OCM engagement for the duration of

project planning, transition, and final implementation phase including:

  i. Designing and managing team structures with roles and responsibilities to facilitate automated program delivery, while noting any risks anticipated from the lack of readiness in the organization and staffing.
  ii. Ensure a successful transition for the integration of new processes and technology with stakeholders.
  iii. Organizational readiness assessment

P, N, Q, or **I** & Notes:

3. Disaster Recovery

a. ☐Availability of ninety-nine-point nine percent (99.9%) of uptime
b. ☐Capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six (6) hours (i.e., maximum data loss cannot exceed six (6) hours)
c. ☐Recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours.

P, **N**, Q, or I & Notes:
No mention of socure

4. Feature Enhancements

a. ☒The State is seeking two hundred and fifty (250) hours of time and material for each proposed technology (CIAM), Personalized Dashboard, Disclosure and Consent Management, Data Management, and Recommendation Technology) to allow for specifications and enhancements during the contract period.

P, N, Q, or **I** & Notes:
No more than 40 hours

5. Project Management

a. ☐The State plans to have its own project manager however, the awarded Bidder must have a project manager that has the primary responsibility for executing the project management tasks associated with the project. The awarded Bidder will:
   i. Work in collaboration with the State's Project Manager
   ii. Align with State Project Management processes and practices.
b. ☒Manage the implementation, executing all activities, tasks, deliverables and resource needs, both state and awarded Bidder.

c. ☒Track project status including managing and tracking all project risks, issues and decisions.
d. ☒Track and report status of deliverables and project status
e. ☐The awarded Bidder will provide their approach for project management and administration services including:
    i. Project Management Methodology
    ii. Project Governance
    iii. Resource Allocation and Schedule Management approach
    iv. Communication Management Approach including status reporting and document repository management.
    v. Risk and Issue Management Methodology
    vi. Change Management Methodology
    vii. Quality Management Methodology

P, **N**, Q, or I & Notes:

Does not cover all requirements noted above

D. Value Added Options (Other)

☒Bidders shall provide value added optional services to address relevant matters that have not been anticipated in this RFP but contribute to successful implementation of the proposed solutions, as well as any technology or services that will reduce risk to the project’s quality and continuity. The value-added technology and services will not be included in the evaluation process but may be added during the contract negotiations.

P, N, Q, or **I** & Notes:

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Microsoft
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

Section I – Preliminary Information (No points – Eligibility Requirements)

(File #1 App. A, B, C)
☒Done – Pass/Fail by Procurement & RFP Coordinator

Section II Organization Qualifications and Experience

(File #2 – App. D, E + other areas that have no Appendix number but are part of File #2)

1. **Overview of the Organization (App. D)**
   ☒Bidders must include three examples of projects which demonstrate their experience and expertise in performing these services as well as highlighting the Bidder's stated qualifications and skills.

   Statement of qualifications
   ☒Client name, contact person, Ph#, email.
   Contract history with the state may be considered in rating proposals even if not provided by the bidder.

   P, N, Q, or I & Notes:Q no contact information provided

2. **Subcontractors (App. E)**
   ☒If subcontractors are to be used, Bidders must provide the name, address, phone number, contact person, and a brief description of the subcontractors' organizational capacity and qualifications.
   Business name, contact person, address, ph#, email.
   P, N, Q, or I & Notes:P

3. **Organizational Chart (No Appendix)**
   ☒Bidders must provide an organizational chart. The organizational chart must include the project being proposed. Each position must be identified by position title and corresponding to the personnel job descriptions.
   P, N, Q, or I & Notes:P

4. **Litigation (No App.)**

☒Bidders must attach a list of all current litigation in which the Bidder is named and a list of all closed cases that have closed within the past five (5) years in which the Bidder paid the claimant either as part of a settlement or by decree. For each, list the entity bringing suit, the complaint, the accusation, amount, and outcome.
P, N, Q, or I & Notes:P

5. **Financial Viability (No App.)**
☒Bidders must provide a current copy of their Dun & Bradstreet Business Information Report Snapshot.
P, N, Q, or I - Notes:P

6. **Licensure/Certification (No App.)**
☒Bidders *may* provide documentation of any applicable licensure/certification or specific credentials that are related to providing the proposed services of the RFP.
P, N, Q, or I & Notes:P

7. **Certificate of Insurance (No App.)**
☒Bidders must provide a certificate of insurance on a standard ACORD form (or the equivalent) evidencing the Bidder's general liability, professional liability and any other relevant liability insurance policies that might be associated with the proposed services.
P, N, Q, or I & Notes:Q says added below but don't see

Section III - Proposed Services
(File #3 – App. F, G, H)

1. **Technical Assessment (App. F)**
☒Done

2. **Services to be Provided (App. G)**

Note: on App. G Detailed Technical and Functional Requirements Excel spreadsheet, a tab is labeled User Stories. No response is required for Tab 3; these were provided to bidders for clarity and understanding of the expected journey a Constituent will experience.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Microsoft
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes:P	**1. System security components System security must include the following security components:**
	1) Account Take Over Protections
	a) Account Sign-in Protections
	a) Account Sign-in Protections
	a) Adaptive AI Technology
	b) Bot Protection: identify visitor behavior through analysis of technical and behavioral data.
☒ P, Q, N or I Notes: P	**2. Identity Proofing must have the ability to provide levels of proofing which will be directly tied to the constituent's level of access.**
	1) Define various levels of id proofing
	2) Document Image Capture
	3) Close coupling with authentication
☒ P, Q, N or I Notes: P	**3. Multi-factor authentication The system must support multi-factor authentication to protect against user impersonation and credential theft.**
☒ P, Q, N or I Notes: P	**4. Risk-based factors The system must support risk-based factors and scores that are based on factors such as, but not limited to, device and location.**
☒ P, Q, N or I Notes: P No deprovision mentioned	**5. Identity lifecycle management components The system must include the following identity lifecycle management components for risk-based critical applications not limited to end users but also for generic accounts and system/service accounts:**
P	1) Identity Creation
P	2) Identity provisioning
P	3) Attribute maps
P	4) Authentication (e.g., password policies and synchronization)

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Microsoft
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes:P	**6. Security event logging The system must log security information and events.**
	Security Information and Event Management (SIEM) – Splunk
	Cloud Services: Azure, AWS, Oracle, Google
☒ P, Q, N or I Notes:P	**7. Security Certifications The system must comply too or have the following security certifications:**
P	1) NIST 800-53
P	2) FedRamp
P	3) HIPAA
P	4) SOC 2 Type II
	Note:
P	IRS require a 45-day letter approval for new cloud solutions.
☒ P, Q, N or I Notes:P	**8. SIEM (Splunk) integration The system must be able to integrate with the State of Maine Security Information and Event Monitoring (SIEM) Splunk for Security Operations Center operations.**
☒ P, Q, N or I Notes:P	**9. Core constituent data. The system must maintain a central repository of basic (core) constituent data, that can be used by any SoM application to reduce data redundancy and outdated or inaccurate information while maintaining confidentiality.**
☒ P, Q, N or I Notes:P	**11. Data Management. The system must apply the Data Management Rules to the constituent profile data as per the SoM Data Management Policies.**
☒ P, Q, N or I Notes:P	**12. SOM Employee. The system must support multiple identities for SOM employees that work with the portal in a support role.**

P	1) SOM Employee identity and credentials for supporting the application.
P	2) Constituent identity and credentials to use the state services offered through the portal.

☒ P, Q, N or I Notes:P	**13. APIs. The system must be able to connect to at least one agency application.**
	Considerations:
	a) OpenID, OAuth, WS-Fed, SAML, LDAP, Active Directory, Application Programming Interfaces (APIs), Software Development
	b) Develop once and reuse often with other agencies would be ideal
☒ P, Q, N or I Notes:P	**14. User identification matching. The system must be able to match the identity of the portal user to the identity of the same user in the agency system.**
☒ P, Q, N or I Notes:P	**15. Single sign-on. The system must support single sign-on to the agency application.**
☒ P, Q, N or I Notes:P	**16. Import user profile data from agency systems. The system must be able to import user data from different SoM applications to ensure offboarding happens in a timely manner, so that government resources are protected from fraud. (example: death records)**
☒ P, Q, N or I Notes:P	**17. History logging.** 1) The system must log all actions taken by:
P	a) Constituents
P	b) MaineIT support
	Including but not limited to:
P	c) who made the change

P	d) when the change was made
P	e) what changed
☒ P, Q, N or I Notes:P	**18. Reporting. The logging data (history) must be available for constituent and system dashboards and reporting in general.**
☒ P, Q, N or I Notes:P	**19. Security Controls. The system must comply to the following security controls:**
P	1) DDOS Protections[WN1] ,
P	2) OWASP Top 10
P	a) Cross Site Scripting,
P	b) SQL Injection,
P	3) Authentication bypass,
P	a) poorly authenticated APIs,
P	b) Role based access controls,
P	c) proper session control
P	4) Real-time visibility,
P	5) Anomalous behavior,
P	6) User sign with geo-location tracking,
P	Geo-blocking capabilities.
P	Security controls must include Web Application Firewall [WN1]
☒ P, Q, N or I Notes:P	**20. General System Requirements.** 1) Mobile Support with Native App; (iOS and Android)
P	2) System availability: 24/7 with 4x1-hour outages per year
P	3) Identity relationships must be tracked in the cloud infrastructure.
P	4) Support responsive web and web browsers.
P	a. Supports Windows, Chrome, and Macintosh operating systems
☒	**21. Training and Support.**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Microsoft
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

P, Q, N or I Notes:P	1) Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
P	2) MaineIT will require technical/administrator training. There will be initial training and on-going training as users are added.
P	3) Have a continuous process to ensure constituents that may have run into issues setting up accounts can have help 24/7.
☒ P, Q, N or I Notes:P	**22. Support Requirements** 1) The Bidder will provide support, and maintenance for the solution to begin immediately after receiving the State's official acceptance of the implemented solution.
P	2) Support and maintenance will be provided for the terms and duration specified in the contract.
P	3) The Bidder will address all questions and reported problems related to the technical and functional operation of the system.
P	4) The Bidder must provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours: 8:00 a.m. to 5:00 p.m. Eastern Standard Time.
P	5) As part of the maintenance agreement, the Bidder will make all product releases and upgrades available to the State at no additional charge.
P	6) All release and upgrades shall be implemented and tested by the Bidder, outside of the normal operating hours of the State government.
P	7) User testing shall occur during normal State business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State government.
☒ P, Q, N or I Notes:P	**23. Hosting** Solution can comply with MaineIT remote hosting policies. a) Remote Hosting Policy http://maine.gov/oit/policies/RemoteHostingPolicy.pdf b) Hosting Customization Policy http://maine.gov/oit/policies/HostingCustomizationPolicy.pdf
☒ P, Q, N or I	**24. Disaster Recovery** Proposed Solution can comply with MaineIT security requirements and remote hosting requirements, without requiring waivers, before contract finalization.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Microsoft
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

Notes:P	
P	1) Maintaining an availability metric of ninety-nine-point nine percent (99.9%) of uptime
P	2) Ensuring the capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six hours (i.e., maximum data loss cannot exceed six (6) hours);
P	3) Ensuring a recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours;
Q	4) Ensuring the hosting environment provides adequate capacity to ensure that, under ethernet connectivity to the client device, data inquiry/lookup response is within three (3) seconds, and data modification response is within five (5) seconds;
P	5) Providing the Department at least thirty (30) calendar day advance written notice of any material change in network operations or architecture;
P	6) Ensuring any planned material change in network operations or architecture cannot be made without the prior written consent of the Department; and Outlining of all Service Level Agreements (SLAs) for technical support (the awarded Bidder shall be open to negotiation to ensure the SLAs meet the Department's needs

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

☒1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
P, N, Q, or I & Notes:P

☒1b) Detailed description of the technologies, software and / or hardware for each of the components.
P, N, Q, or I & Notes:P

☒1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.

P, N, Q, or I & Notes:P

☒1d) Description of the overall platform and architecture of the proposed solution(s).
P, N, Q, or I & Notes:P

☒1e) Description of any third-party software or partnerships required for the proposed Solution(s).
P, N, Q, or I & Notes:P

☒2a) A detailed timeline and description of milestones, deliverables, tasks
P, N, Q, or I & Notes:P

☒2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period
P, N, Q, or I & Notes:P resumes to be provided upon award of contract

☒2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
P, N, Q, or I & Notes:P

☒2d) Average time to market for each component.
P, N, Q, or I & Notes:Q needs discover for average

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. ☒Capture Constituent Identity and profile data.

P, N, Q, or I & Notes:P

b. ☒Provide identity provisioning and deprovisioning.
P, N, Q, or I & Notes:Q deprovisioning

c. ☒Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
   i. Identity Creation
   ii. Identity provisioning
   iii. Attribute maps
   iv. Authentication (e.g., password policies and synchronization)
   P, N, Q, or I & Notes:P

d. ☒Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies.
P, N, Q, or I & Notes:P

e. ☒Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
P, N, Q, or I & Notes:P

f. ☒Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.
P, N, Q, or I & Notes:P

g. ☒Allow for multiple role selections for the following identities:
   i. Individual
   ii. Business Owner
   iii. Support multiple identities for State employees that work with the portal in a support role:
      (a) SOM Employee identity and credentials for supporting the application.
      (b) Constituent identity and credentials to use the state services offered through the portal.
   iv. Multi role individual (Individual and Business Owner)
   P, N, Q, or I & Notes:P

h. ☒Have the ability to provide levels of proofing which will be directly tied to the Constituent’s level of consent given.
P, N, Q, or I & Notes:P

i. ☒Support multi-factor authentication to protect against user impersonation and credential theft.
P, N, Q, or I & Notes:P

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Microsoft
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

B.2. ☒The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.
P, N, Q, or I & Notes:P

a. Disclosure and Consent Management

The desire of the State is to be as transparent as possible and respect the privacy of the individual interacting with the Constituents' Portal. Consent is a core tenant of maintaining the public trust in the Constituents' Portal and will be a foundational component of the architecture.

The Disclosure and Consent Management solution shall include:

i. ☒Granular consent management that encompasses the automated functions necessary to create, modify, revoke, and manage Constituent consents.
ii. ☒Allow users the ability to opt-in and opt-out of data sharing and services within the Constituents' portal.
iii. ☒Obtain user consent both in an interactive and set preference mode for a variety of transactions on the Portal.
iv. ☒Support administrative users' management of standard legal disclaimers and data classification for transactions.
v. ☒Highly configurable with version control and history tracking for consent language.
vi. ☒Ability for end user to access a retrievable log of granted consent and data usage on the portal derived from the consent.

P, N, Q, or I & Notes:P

b. Recommendation Technology

The State is seeking options which, while maintaining individual privacy, will collect and analyze data about user interactions, behavior, and preferences. The

expected outcome of this will be to provide insights and intelligence that help the State make informed decisions and improve Constituent experiences.

i. ☒From the user perspective, the portal should be able to make real-time recommendations for related services.
ii. ☒Data captured in this environment must be obfuscated, as to not allow any party to directly target or track the preferences of an individual or their usage of the portal.
iii. ☒Solution providers should discuss in detail their use, storage, destruction of metadata, and tracking technologies with emphasis on how their offering provides analytical insights while protecting the individual user privacy.

P, N, Q, or I & Notes:Q destruction meta data

c. Data Management

The State is seeking the ability for the portal's Constituent identity to be linked to records maintained by individual State agencies. The proposed solution will include:

i. ☒Capabilities to streamline the sharing of data between State systems, including
    i. The identity assurance level
    ii. Agency to user notifications
    iii. Verification of user consent
    iv. Identity resolution
    v. Data sharing between agencies.
ii. ☒Maintain a central repository of basic (core) Constituent data, that can be used by any State application to reduce data redundancy, and outdated or inaccurate information while maintaining confidentiality.
iii. ☒Ability to integrate with State applications using, OpenID, OAuth, Web Services Federation Protocol (WS-Fed), Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), Active Directory, Application Programming Interface (API) or equivalent protocols.
iv. ☒Ability to match the identity of the portal user to the identity of the same user in the Agency system.
v. ☒Log all actions taken by:
    i. Constituents
    ii. MaineIT Support, including:
        (a) Who made the change
        (b) When the change was made

(c) What changed to and from

vi. ☒Logging data must be available for system dashboards and reporting.

P, N, Q, or I & Notes:P

d. Customer Service

The State is seeking solution(s) to provide 24/7/365 customer service to Constituents regardless of their location or technical abilities.

i. ☒Support Constituents with personalized and timely assistance.
ii. ☒Provide the state options to support our Constituents across multiple channels including, but not limited to phone, email, chat, etc.

P, N, Q, or I & Notes: Q Phone support

C.1. General System

a. ☒Mobile support with native app (iOS and Android)
b. ☒System availability: 24/7 with a maximum of four (4) 1-hour outages per year
c. ☒Identity relationships must be tracked in the cloud infrastructure.
d. ☒Support responsive web and web browsers.
   i. ☒Supports Windows, Chrome, and Macintosh operating systems.

P, N, Q, or I & Notes:P

C.2. ☒Compliance with MaineIT Policies & Standards

a. Architecture Compliance Policy
b. System and Services Acquisition Policy and Procedures (SA-1)
c. Application Deployment Certification Policy
d. Digital Accessibility Policy
e. Remote Hosting Policy
f. Data Exchange Policy
g. Information Security Policy
h. Access Control Policy (AC-1)
i. Access Control Procedures for Users (AC-2)
j. Risk Assessment Policy and Procedures (RA-1)
k. Vulnerability Scanning Procedure (RA-5)
l. Security Assessment and Authorization Policy and Procedures (CA-1)
m. System and Information Integrity Policy and Procedures (SI-1)

n. Configuration Management Policy (CM-1)
o. Web Standards

P, N, Q, or I & Notes:P

C.3. Support and Maintenance

a. ☒Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State's official acceptance of the implemented solution.
   P, N, Q, or I & Notes:P
b. ☒Terms and duration of the support and maintenance will be specified in the contract.
   P, N, Q, or I & Notes:P

c. ☒All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
   P, N, Q, or I & Notes:P
d. ☒Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
   P, N, Q, or I & Notes:Q toll free number
e. ☒All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
   P, N, Q, or I & Notes:P
f. ☒All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
   P, N, Q, or I & Notes:P
g. ☒User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
   P, N, Q, or I & Notes:P

4. Security

The proposed solutions must provide a robust security system that aligns with the States Security Policies, standards, and Processes, Including:

Comply with or have the following security certifications:

i. ☒National Institute of Standards and Technology (NIST) 800-53
ii. ☒FedRamp
iii. ☒Health Insurance Portability and Accountability Act (HIPAA)
iv. ☒SOC 2 Type II
v. ☒Comply to the following security controls:
vi. ☒DDOS Protections [WN1]
vii. ☒Open Web Application Security Project (OWASP) Top 10
viii. ☒Cross Site Scripting
ix. ☒Structured Query Language (SQL) Injection
x. ☒Authentication bypass
xi. ☒Poorly authenticated APIs
xii. ☒Role based access controls
xiii. ☒Proper session control
xiv. ☒Real-time visibility
xv. ☒Anomalous behavior
xvi. ☒User sign with geo-location tracking
xvii. ☒Geo-blocking capabilities.
xviii. ☒Web Application Firewall [WN1]
xix. ☒System security must include the following security components:
xx. ☒Account take over protections
xxi. ☒Account sign-in Protections
xxii. ☒Behavior detection and evaluation
xxiii. ☒Adaptive AI Technology
xxiv. ☒Bot Protection; identity visitor behavior through analysis, technical and behavioral data.
xxv. ☒The proposed solution must be able to integrate with the State Security Information and Event Monitoring (SIEM) Splunk. Ability to log security information and events.

P, N, Q, or I & Notes:P

5. Licensing

☒The State is aware that multiple licensing options are available and will be required to support the proposed solution in its entirety. The State seeks bids which will provide the most cost-effective licensing approach. Bidders are required to provide a detail breakdown for the proposed licensing.

P, N, Q, or I & Notes:P

1. Training and OCM (Organizational Change Management)

a. ☒Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
b. ☒Training must include technical and administrator training, initial and ongoing as users are added.
c. ☒Continuous process to ensure Constituents that may have run into issues setting up accounts have help 24/7.
d. ☒Bidders shall guide the State in OCM engagement for the duration of project planning, transition, and final implementation phase including:
   i. Designing and managing team structures with roles and responsibilities to facilitate automated program delivery, while noting any risks anticipated from the lack of readiness in the organization and staffing.
   ii. Ensure a successful transition for the integration of new processes and technology with stakeholders.
   iii. Organizational readiness assessment

P, N, Q, or I & Notes:P

3. Disaster Recovery

a. ☒Availability of ninety-nine-point nine percent (99.9%) of uptime
b. ☒Capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six (6) hours (i.e., maximum data loss cannot exceed six (6) hours)
c. ☒Recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours.

P, N, Q, or I & Notes:P

4. Feature Enhancements

a. ☒The State is seeking two hundred and fifty (250) hours of time and material for each proposed technology (CIAM), Personalized Dashboard, Disclosure and Consent Management, Data Management, and Recommendation Technology) to allow for specifications and enhancements during the contract period.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Microsoft
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

P, N, Q, or I & Notes:

5. Project Management

a. ☒The State plans to have its own project manager however, the awarded Bidder must have a project manager that has the primary responsibility for executing the project management tasks associated with the project. The awarded Bidder will:
   i. Work in collaboration with the State's Project Manager
   ii. Align with State Project Management processes and practices.
b. ☒Manage the implementation, executing all activities, tasks, deliverables and resource needs, both state and awarded Bidder.
c. ☒Track project status including managing and tracking all project risks, issues and decisions.
d. ☒Track and report status of deliverables and project status
e. ☒The awarded Bidder will provide their approach for project management and administration services including:
   i. Project Management Methodology
   ii. Project Governance
   iii. Resource Allocation and Schedule Management approach
   iv. Communication Management Approach including status reporting and document repository management.
   v. Risk and Issue Management Methodology
   vi. Change Management Methodology
   vii. Quality Management Methodology

P, N, Q, or I & Notes:P

D. Value Added Options (Other)

☒Bidders shall provide value added optional services to address relevant matters that have not been anticipated in this RFP but contribute to successful implementation of the proposed solutions, as well as any technology or services that will reduce risk to the project's quality and continuity. The value-added technology and services will not be included in the evaluation process but may be added during the contract negotiations.

P, N, Q, or I & Notes:P #11 like service solution

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Microsoft
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Microsoft
DATE: 05 June 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: MaineIT

Section I – Preliminary Information (No points – Eligibility Requirements)

(File #1 App. A, B, C)

☒Done – Pass/Fail by Procurement & RFP Coordinator

Section II Organization Qualifications and Experience

(File #2 – App. D, E + other areas that have no Appendix number but are part of File #2)

1. **Overview of the Organization (App. D)**
   ☒Bidders must include three examples of projects which demonstrate their experience and expertise in performing these services as well as highlighting the Bidder's stated qualifications and skills.
   P: Strong response
   Q: Four examples, instead of three

   Statement of qualifications
   ☐Client name, contact person, Ph#, email.
      Contract history with the state may be considered in rating proposals even if not provided by the bidder.
      N: Did NOT respond
      P: Conract history w/ the State

2. **Subcontractors (App. E)**
   ☒If subcontractors are to be used, Bidders must provide the name, address, phone number, contact person, and a brief description of the subcontractors' organizational capacity and qualifications.
   Business name, contact person, address, ph#, email.
      P: Two subcontractors (WhoIAm & NewEraTech). All details provided.

3. **Organizational Chart (No Appendix)**
   ☒Bidders must provide an organizational chart. The organizational chart must include the project being proposed. Each position must be identified by position title and corresponding to the personnel job descriptions.
      P: Strong response

4. **Litigation (No App.)**
   ☒Bidders must attach a list of all current litigation in which the Bidder is named and a list of all closed cases that have closed within the past five (5) years in which the

Bidder paid the claimant either as part of a settlement or by decree. For each, list the entity bringing suit, the complaint, the accusation, amount, and outcome.
P: Strong response

5. **Financial Viability (No App.)**
☒Bidders must provide a current copy of their Dun & Bradstreet Business Information Report Snapshot.
N: Could NOT locate the D&B Snapshot
P: Otherwise, strong response

6. **Licensure/Certification (No App.)**
☒Bidders *may* provide documentation of any applicable licensure/certification or specific credentials that are related to providing the proposed services of the RFP.
P: Strong response

7. **Certificate of Insurance (No App.)**
☒Bidders must provide a certificate of insurance on a standard ACORD form (or the equivalent) evidencing the Bidder's general liability, professional liability and any other relevant liability insurance policies that might be associated with the proposed services.
N: Could NOT locate

Section III - Proposed Services

(File #3 – App. F, G, H)

1. **Technical Assessment (App. F)**
☒Done

2. **Services to be Provided (App. G)**

Note: on App. G Detailed Technical and Functional Requirements Excel spreadsheet, a tab is labeled User Stories. No response is required for Tab 3; these were provided to bidders for clarity and understanding of the expected journey a Constituent will experience.

☒ *P: Adequate response*	**1. System security components System security must include the following security components:**
	1) Account Take Over Protections
	a) Account Sign-in Protections

	a) Account Sign-in Protections
	a) Adaptive AI Technology
	b) Bot Protection: identify visitor behavior through analysis of technical and behavioral data.
☒ *P: Adequate response*	**2. Identity Proofing must have the ability to provide levels of proofing which will be directly tied to the constituent's level of access.**
	1) Define various levels of id proofing
	2) Document Image Capture
	3) Close coupling with authentication
☒ *P: Adequate response*	**3. Multi-factor authentication The system must support multi-factor authentication to protect against user impersonation and credential theft.**
☒ *P: Adequate response*	**4. Risk-based factors The system must support risk-based factors and scores that are based on factors such as, but not limited to, device and location.**
☒ *P: Adequate response*	**5. Identity lifecycle management components The system must include the following identity lifecycle management components for risk-based critical applications not limited to end users but also for generic accounts and system/service accounts:**
	1) Identity Creation
	2) Identity provisioning
	3) Attribute maps
	4) Authentication (e.g., password policies and synchronization)
☒ *N: Weak response. Covers native stack, but NOT Socure*	**6. Security event logging The system must log security information and events.**
	Security Information and Event Management (SIEM) – Splunk

	Cloud Services: Azure, AWS, Oracle, Google
☒ *N: Weak response. Covers native stack, but NOT Socure* *P: Ack of the IRS 45-day notice.*	**7. Security Certifications The system must comply too or have the following security certifications:**
	1) NIST 800-53
	2) FedRamp
	3) HIPAA
	4) SOC 2 Type II
	Note:
	IRS require a 45-day letter approval for new cloud solutions.
☒ *N:Weak response. Covers native stack, but NOT Socure*	**8. SIEM (Splunk) integration The system must be able to integrate with the State of Maine Security Information and Event Monitoring (SIEM) Splunk for Security Operations Center operations.**
☒ *P: Adequate response*	**9. Core constituent data. The system must maintain a central repository of basic (core) constituent data, that can be used by any SoM application to reduce data redundancy and outdated or inaccurate information while maintaining confidentiality.**
☒ *P: Adequate response*	**11. Data Management. The system must apply the Data Management Rules to the constituent profile data as per the SoM Data Management Policies.**
☒ *P: Strong response*	**12. SOM Employee. The system must support multiple identities for SOM employees that work with the portal in a support role.**
	1) SOM Employee identity and credentials for supporting the application.
	2) Constituent identity and credentials to use the state services offered through the portal.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Microsoft
DATE: 05 June 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: MaineIT

☒ *P: Adequate response*	**13. APIs. The system must be able to connect to at least one agency application.**
	Considerations:
	a) OpenID, OAuth, WS-Fed, SAML, LDAP, Active Directory, Application Programming Interfaces (APIs), Software Development
	b) Develop once and reuse often with other agencies would be ideal
☒ *P: Adequate response*	**14. User identification matching. The system must be able to match the identity of the portal user to the identity of the same user in the agency system.**
☒ *P: Adequate response*	**15. Single sign-on. The system must support single sign-on to the agency application.**
☒ *P: Adequate response*	**16. Import user profile data from agency systems. The system must be able to import user data from different SoM applications to ensure offboarding happens in a timely manner, so that government resources are protected from fraud. (example: death records)**
☒ *N: Weak response (Unclear if it covers both Azure & Socure)*	**17. History logging.** 1) The system must log all actions taken by:
	a) Constituents
	b) MaineIT support
	Including but not limited to:
	c) who made the change
	d) when the change was made

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Microsoft
DATE: 05 June 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: MaineIT

	e) what changed
☒ *N: Weak response (Unclear if it covers both Azure & Socure)*	**18. Reporting. The logging data (history) must be available for constituent and system dashboards and reporting in general.**
☒ *N: Weak response (Covers Azure, but NOT Socure)*	**19. Security Controls. The system must comply to the following security controls:**
	1) DDOS Protections[WN1] ,
	2) OWASP Top 10
	a) Cross Site Scripting,
	b) SQL Injection,
	3) Authentication bypass,
	a) poorly authenticated APIs,
	b) Role based access controls,
	c) proper session control
	4) Real-time visibility,
	5) Anomalous behavior,
	6) User sign with geo-location tracking,
	Geo-blocking capabilities.
	Security controls must include Web Application Firewall [WN1]
☒ *P: Adequate response*	**20. General System Requirements.** 1) Mobile Support with Native App; (iOS and Android)
	2) System availability: 24/7 with 4x1-hour outages per year
	3) Identity relationships must be tracked in the cloud infrastructure.

	4) Support responsive web and web browsers.
	a. Supports Windows, Chrome, and Macintosh operating systems
☒ *P: Adequate response (Details at discovery)*	**21. Training and Support.** 1) Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
	2) MaineIT will require technical/administrator training. There will be initial training and on-going training as users are added.
	3) Have a continuous process to ensure constituents that may have run into issues setting up accounts can have help 24/7.
☒ *P: Adequate response (Details at discovery)*	**22. Support Requirements** 1) The Bidder will provide support, and maintenance for the solution to begin immediately after receiving the State's official acceptance of the implemented solution.
	2) Support and maintenance will be provided for the terms and duration specified in the contract.
	3) The Bidder will address all questions and reported problems related to the technical and functional operation of the system.
	4) The Bidder must provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours: 8:00 a.m. to 5:00 p.m. Eastern Standard Time.
	5) As part of the maintenance agreement, the Bidder will make all product releases and upgrades available to the State at no additional charge.
	6) All release and upgrades shall be implemented and tested by the Bidder, outside of the normal operating hours of the State government.
	7) User testing shall occur during normal State business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State government.
☒	**23. Hosting**

N: Weak response (Covers Azure, but NOT Socure)	Solution can comply with MaineIT remote hosting policies. a) Remote Hosting Policy http://maine.gov/oit/policies/RemoteHostingPolicy.pdf b) Hosting Customization Policy http://maine.gov/oit/policies/HostingCustomizationPolicy.pdf
☒ *P: Adequate response*	**24. Disaster Recovery** Proposed Solution can comply with MaineIT security requirements and remote hosting requirements, without requiring waivers, before contract finalization.
	1) Maintaining an availability metric of ninety-nine-point nine percent (99.9%) of uptime
	2) Ensuring the capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six hours (i.e., maximum data loss cannot exceed six (6) hours);
	3) Ensuring a recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours;
	4) Ensuring the hosting environment provides adequate capacity to ensure that, under ethernet connectivity to the client device, data inquiry/lookup response is within three (3) seconds, and data modification response is within five (5) seconds;
	5) Providing the Department at least thirty (30) calendar day advance written notice of any material change in network operations or architecture;
	6) Ensuring any planned material change in network operations or architecture cannot be made without the prior written consent of the Department; and Outlining of all Service Level Agreements (SLAs) for technical support (the awarded Bidder shall be open to negotiation to ensure the SLAs meet the Department's needs

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

☒1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
P: Strong response

☒1b) Detailed description of the technologies, software and / or hardware for each of the components.
P: Strong response

☒1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.
P: Strong response

☒1d) Description of the overall platform and architecture of the proposed solution(s).
P: Strong response

☒1e) Description of any third-party software or partnerships required for the proposed Solution(s).
P: Strong response

☒2a) A detailed timeline and description of milestones, deliverables, tasks
P: Adequate response

☒2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period
P: Adequate response

☒2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
P: Adequate response

☒2d) Average time to market for each component.
P: Adequate response

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. ☒Capture Constituent Identity and profile data.
   P: Strong response

b. ☒Provide identity provisioning and deprovisioning.

P: Strong response

c. ☒Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
   i. Identity Creation
   ii. Identity provisioning
   iii. Attribute maps
   iv. Authentication (e.g., password policies and synchronization)
   P: Strong response

d. ☒Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies.
P: Strong response

e. ☒Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
P: Strong response

f. ☐Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.
N: NO response

g. ☐Allow for multiple role selections for the following identities:
   i. Individual
   ii. Business Owner
   iii. Support multiple identities for State employees that work with the portal in a support role:
      (a) SOM Employee identity and credentials for supporting the application.
      (b) Constituent identity and credentials to use the state services offered through the portal.
   iv. Multi role individual (Individual and Business Owner)
N: NO response

h. ☐Have the ability to provide levels of proofing which will be directly tied to the Constituent's level of consent given.
N: NO response

i. ☒Support multi-factor authentication to protect against user impersonation and credential theft.
P: Adequate response

B.2. ☒The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.
P: Strong response

a. Disclosure and Consent Management
The desire of the State is to be as transparent as possible and respect the privacy of the individual interacting with the Constituents' Portal. Consent is a core tenant of maintaining the public trust in the Constituents' Portal and will be a foundational component of the architecture.
The Disclosure and Consent Management solution shall include:

i. ☒Granular consent management that encompasses the automated functions necessary to create, modify, revoke, and manage Constituent consents.
P: Adequate response

ii. ☒Allow users the ability to opt-in and opt-out of data sharing and services within the Constituents' portal.
P: Adequate response

iii. ☒Obtain user consent both in an interactive and set preference mode for a variety of transactions on the Portal.
P: Adequate response

iv. ☒Support administrative users' management of standard legal disclaimers and data classification for transactions.
P: Adequate response

v. ☐Highly configurable with version control and history tracking for consent language.
N: NO response

vi. ☐Ability for end user to access a retrievable log of granted consent and data usage on the portal derived from the consent.
N: NO response

b. Recommendation Technology

The State is seeking options which, while maintaining individual privacy, will collect and analyze data about user interactions, behavior, and preferences. The expected outcome of this will be to provide insights and intelligence that help the State make informed decisions and improve Constituent experiences.

i. ☒From the user perspective, the portal should be able to make real-time recommendations for related services.
P: Strong response

ii. ☐Data captured in this environment must be obfuscated, as to not allow any party to directly target or track the preferences of an individual or their usage of the portal.
N: NO response

iii. ☐Solution providers should discuss in detail their use, storage, destruction of metadata, and tracking technologies with emphasis on how their offering provides analytical insights while protecting the individual user privacy.
N: NO response

c. Data Management

The State is seeking the ability for the portal’s Constituent identity to be linked to records maintained by individual State agencies. The proposed solution will include:

i. ☒Capabilities to streamline the sharing of data between State systems, including
    i. The identity assurance level
    ii. Agency to user notifications
    iii. Verification of user consent
    iv. Identity resolution
    v. Data sharing between agencies.
    P: Adequate response

ii. ☒Maintain a central repository of basic (core) Constituent data, that can be used by any State application to reduce data redundancy, and outdated or inaccurate information while maintaining confidentiality.
P: Adequate response

iii. ☒Ability to integrate with State applications using, OpenID, OAuth, Web Services Federation Protocol (WS-Fed), Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), Active Directory, Application Programming Interface (API) or equivalent protocols.
P: Adequate response

iv. ☐Ability to match the identity of the portal user to the identity of the same user in the Agency system.
N: NO response

v. ☒Log all actions taken by:
  i. Constituents
  ii. MaineIT Support, including:
    (a) Who made the change
    (b) When the change was made
    (c) What changed to and from
P: Adequate response

vi. ☒Logging data must be available for system dashboards and reporting.
P: Adequate response

d. Customer Service
The State is seeking solution(s) to provide 24/7/365 customer service to Constituents regardless of their location or technical abilities.
  i. ☒Support Constituents with personalized and timely assistance.
  ii. ☒Provide the state options to support our Constituents across multiple channels including, but not limited to phone, email, chat, etc.
P: Adequate response
Q: Was it included in the Cost Proposal?

C.1. General System
a. ☒Mobile support with native app (iOS and Android)

b. ☒System availability: 24/7 with a maximum of four (4) 1-hour outages per year
c. ☒Identity relationships must be tracked in the cloud infrastructure.
d. ☒Support responsive web and web browsers.
    i. ☒Supports Windows, Chrome, and Macintosh operating systems.

P: Adequate responses

C.2. ☒Compliance with MaineIT Policies & Standards
a. Architecture Compliance Policy
b. System and Services Acquisition Policy and Procedures (SA-1)
c. Application Deployment Certification Policy
d. Digital Accessibility Policy
e. Remote Hosting Policy
f. Data Exchange Policy
g. Information Security Policy
h. Access Control Policy (AC-1)
i. Access Control Procedures for Users (AC-2)
j. Risk Assessment Policy and Procedures (RA-1)
k. Vulnerability Scanning Procedure (RA-5)
l. Security Assessment and Authorization Policy and Procedures (CA-1)
m. System and Information Integrity Policy and Procedures (SI-1)
n. Configuration Management Policy (CM-1)
o. Web Standards

N: Weak response (Covers native stack, but NOT Socure)

C.3. Support and Maintenance
a. ☒Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State’s official acceptance of the implemented solution.
N: Weak response (Covers native stack, but NOT Socure)

b. ☒Terms and duration of the support and maintenance will be specified in the contract.
N: Weak response (Covers native stack, but NOT Socure)

c. ☒All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
N: Weak response (Covers native stack, but NOT Socure)

d. ☒Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
N: Weak response (Covers native stack, but NOT Socure)

e. ☒All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
N: Weak response (Covers native stack, but NOT Socure)

f. ☒All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
N: Weak response (Covers native stack, but NOT Socure)

g. ☒User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
N: Weak response (Covers native stack, but NOT Socure)

4. Security

The proposed solutions must provide a robust security system that aligns with the States Security Policies, standards, and Processes, Including:

Comply with or have the following security certifications:

i. ☒National Institute of Standards and Technology (NIST) 800-53
ii. ☒FedRamp
iii. ☒Health Insurance Portability and Accountability Act (HIPAA)
iv. ☒SOC 2 Type II
v. ☒Comply to the following security controls:
vi. ☒DDOS Protections [WN1]
vii. ☒Open Web Application Security Project (OWASP) Top 10
viii. ☒Cross Site Scripting
ix. ☒Structured Query Language (SQL) Injection
x. ☒Authentication bypass
xi. ☒Poorly authenticated APIs
xii. ☒Role based access controls
xiii. ☒Proper session control

xiv. ☒Real-time visibility
xv. ☒Anomalous behavior
xvi. ☒User sign with geo-location tracking
xvii. ☒Geo-blocking capabilities.
xviii. ☒Web Application Firewall [WN1]
xix. ☒System security must include the following security components:
xx. ☒Account take over protections
xxi. ☒Account sign-in Protections
xxii. ☒Behavior detection and evaluation
xxiii. ☒Adaptive AI Technology
xxiv. ☒Bot Protection; identity visitor behavior through analysis, technical and behavioral data.
xxv. ☒The proposed solution must be able to integrate with the State Security Information and Event Monitoring (SIEM) Splunk. Ability to log security information and events.

N: Weak response (Covers native stack, but NOT Socure)

5. Licensing

☒The State is aware that multiple licensing options are available and will be required to support the proposed solution in its entirety. The State seeks bids which will provide the most cost-effective licensing approach. Bidders are required to provide a detail breakdown for the proposed licensing.

P: Strong response

1. Training and OCM (Organizational Change Management)

a. ☒Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
b. ☒Training must include technical and administrator training, initial and ongoing as users are added.
c. ☐Continuous process to ensure Constituents that may have run into issues setting up accounts have help 24/7.
d. ☒Bidders shall guide the State in OCM engagement for the duration of project planning, transition, and final implementation phase including:
    i. Designing and managing team structures with roles and responsibilities to facilitate automated program delivery, while noting any risks anticipated from the lack of readiness in the organization and staffing.

    ii. Ensure a successful transition for the integration of new processes and technology with stakeholders.
    iii. Organizational readiness assessment

N: NO response to c
P: Otherwise, Adequate response

3. **Disaster Recovery**
    a. ☒Availability of ninety-nine-point nine percent (99.9%) of uptime
    b. ☒Capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six (6) hours (i.e., maximum data loss cannot exceed six (6) hours)
    c. ☒Recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours.

N: Covers Azure, but NOT Socure

4. **Feature Enhancements**

a. ☒The State is seeking two hundred and fifty (250) hours of time and material for each proposed technology (CIAM), Personalized Dashboard, Disclosure and Consent Management, Data Management, and Recommendation Technology) to allow for specifications and enhancements during the contract period.

P: Adequate response

5. **Project Management**
    a. ☒The State plans to have its own project manager however, the awarded Bidder must have a project manager that has the primary responsibility for executing the project management tasks associated with the project. The awarded Bidder will:
        i. Work in collaboration with the State's Project Manager
        ii. Align with State Project Management processes and practices.
    b. ☒Manage the implementation, executing all activities, tasks, deliverables and resource needs, both state and awarded Bidder.
    c. ☒Track project status including managing and tracking all project risks, issues and decisions.
    d. ☒Track and report status of deliverables and project status
    e. ☐The awarded Bidder will provide their approach for project management and administration services including:
        i. Project Management Methodology
        ii. Project Governance

iii. Resource Allocation and Schedule Management approach
iv. Communication Management Approach including status reporting and document repository management.
v. Risk and Issue Management Methodology
vi. Change Management Methodology
vii. Quality Management Methodology

N: NO response to e

N: Weak response overall

D. Value Added Options (Other)

☒Bidders shall provide value added optional services to address relevant matters that have not been anticipated in this RFP but contribute to successful implementation of the proposed solutions, as well as any technology or services that will reduce risk to the project's quality and continuity. The value-added technology and services will not be included in the evaluation process but may be added during the contract negotiations.

P: One elaborate options

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Microsoft
DATE: 6/3/2-24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

Section I – Preliminary Information (No points – Eligibility Requirements)

(File #1 App. A, B, C)
☒Done – Pass/Fail by Procurement & RFP Coordinator

The cost proposal submitted by Microsoft is a non-binding estimate. The Q&A responses from the State of Maine indicated a number of details "to be determined during the discovery phase", as well as limited information on sizing. Microsoft is unable to consider this a "binding" or "final" proposal

It is important to recognize that our current pricing reflects numerous unknowns and assumptions. Through further discovery and with more detailed information, we believe we will be able to refine our scope and provide more detailed estimates. Given the unknowns, we have added additional risk to our services estimations which increased the overall price. This is our standard process and once we have more information, it is quite common for our price to be reduced.. I.

Section II Organization Qualifications and Experience

(File #2 – App. D, E + other areas that have no Appendix number but are part of File #2)

1. Overview of the Organization (App. D)

☒Bidders must include three examples of projects which demonstrate their experience and expertise in performing these services as well as highlighting the Bidder's stated qualifications and skills. First example did not cover all projects areas. No dashboard, internal MS Sharepoint site. 2nd example, missing two components and is in development, not finished does not have Disclosure/Consent or Customer service. Project 4 still in development.

Statement of qualifications

☒Client name, contact person, Ph#, email.

Contract history with the state may be considered in rating proposals even if not provided by the bidder.

P, N, Q, or I & Notes: N – did not provide contact info

2. Subcontractors (App. E)

☒If subcontractors are to be used, Bidders must provide the name, address, phone number, contact person, and a brief description of the subcontractors' organizational

capacity and qualifications.
Business name, contact person, address, ph#, email.
P, N, Q, or I & Notes: P

3. **Organizational Chart (No Appendix)**
☐Bidders must provide an organizational chart. The organizational chart must include the project being proposed. Each position must be identified by position title and corresponding to the personnel job descriptions.
P, N, Q, or I & Notes:

4. **Litigation (No App.)**
☒Bidders must attach a list of all current litigation in which the Bidder is named and a list of all closed cases that have closed within the past five (5) years in which the Bidder paid the claimant either as part of a settlement or by decree. For each, list the entity bringing suit, the complaint, the accusation, amount, and outcome.
P, N, Q, or I & Notes: N - As of June 30, 2023, we accrued aggregate legal liabilities of $617 million. While we intend to defend these matters vigorously, adverse outcomes that we estimate could reach approximately $600 million in aggregate beyond recorded amounts are reasonably possible. Were unfavorable final outcomes to occur, there exists the possibility of a material adverse impact in our consolidated financial statements for the period in which the effects become reasonably estimable.

5. **Financial Viability (No App.)**
☒Bidders must provide a current copy of their Dun & Bradstreet Business Information Report Snapshot.
P, N, Q, or I - Notes: N – did not provide.

6. **Licensure/Certification (No App.)**
☒Bidders *may* provide documentation of any applicable licensure/certification or specific credentials that are related to providing the proposed services of the RFP.
P, N, Q, or I & Notes: N – did not provide.

7. **Certificate of Insurance (No App.)**
☒Bidders must provide a certificate of insurance on a standard ACORD form (or the equivalent) evidencing the Bidder's general liability, professional liability and any other relevant liability insurance policies that might be associated with the proposed services. N – did not provide.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Microsoft
DATE: 6/3/2-24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

P, N, Q, or I & Notes:

Section III - Proposed Services

(File #3 – App. F, G, H)

1. Technical Assessment (App. F)

☒Done

2. Services to be Provided (App. G)

Note: on App. G Detailed Technical and Functional Requirements Excel spreadsheet, a tab is labeled User Stories. No response is required for Tab 3; these were provided to bidders for clarity and understanding of the expected journey a Constituent will experience.

☒ P, Q, N or I Notes: I – just listed Y and put in box title of software meeting the need but no details.	**1. System security components System security must include the following security components:**
	1) Account Take Over Protections
	a) Account Sign-in Protections
	a) Account Sign-in Protections
	a) Adaptive AI Technology
	b) Bot Protection: identify visitor behavior through analysis of technical and behavioral data.
☒ P, Q, N or I Notes: : I – just listed Y and put in box title of software	**2. Identity Proofing must have the ability to provide levels of proofing which will be directly tied to the constituent's level of access.**

meeting the need but no details.	
	1) Define various levels of id proofing
	2) Document Image Capture
	3) Close coupling with authentication
☒ P, Q, N or I Notes: : I – just listed Y and put in box title of software meeting the need but no details.	**3. Multi-factor authentication The system must support multi-factor authentication to protect against user impersonation and credential theft.**
☒ P, Q, N or I Notes: : I – just listed Y and put in box title of software meeting the need but no details.	**4. Risk-based factors The system must support risk-based factors and scores that are based on factors such as, but not limited to, device and location.**
☒ P, Q, N or I Notes: : I – just listed Y and put in box title of software meeting the	**5. Identity lifecycle management components The system must include the following identity lifecycle management components for risk-based critical applications not limited to end users but also for generic accounts and system/service accounts:**

need but no details.	
	1) Identity Creation
	2) Identity provisioning
	3) Attribute maps
	4) Authentication (e.g., password policies and synchronization)

☒ P, Q, N or I Notes: I – yes on SIEM, only addressed Azure on second line	**6. Security event logging The system must log security information and events.**
	Security Information and Event Management (SIEM) – Splunk
	Cloud Services: Azure, AWS, Oracle, Google
☒ P, Q, N or I Notes: P	**7. Security Certifications The system must comply too or have the following security certifications:**
	1) NIST 800-53
	2) FedRamp
	3) HIPAA
	4) SOC 2 Type II
	Note:
	IRS require a 45-day letter approval for new cloud solutions.
☒ P, Q, N or I	**8. SIEM (Splunk) integration The system must be able to integrate with the State of Maine Security Information and**

Notes: P	**Event Monitoring (SIEM) Splunk for Security Operations Center operations.**
☒ P, Q, N or I Notes: P	**9. Core constituent data. The system must maintain a central repository of basic (core) constituent data, that can be used by any SoM application to reduce data redundancy and outdated or inaccurate information while maintaining confidentiality.**
☒ P, Q, N or I Notes: I – state yes but reply is a restating of the requirement	**11. Data Management. The system must apply the Data Management Rules to the constituent profile data as per the SoM Data Management Policies.**
☒ P, Q, N or I Notes:	**12. SOM Employee. The system must support multiple identities for SOM employees that work with the portal in a support role.**
Q – unsure is this has impact: Identities created using non-privledged email domains can only have non-administrative roles (individual or business).	1) SOM Employee identity and credentials for supporting the application.
	2) Constituent identity and credentials to use the state services offered through the portal.

☐ P, Q, N or I	**13. APIs. The system must be able to connect to at least one agency application.**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Microsoft
DATE: 6/3/2-24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

Notes: I – state yes but reply is a restating of the requirement	
	Considerations:
	a) OpenID, OAuth, WS-Fed, SAML, LDAP, Active Directory, Application Programming Interfaces (APIs), Software Development
	b) Develop once and reuse often with other agencies would be ideal
☒ P, Q, N or I Notes: I – state yes but reply is a restating of the requirement	**14. User identification matching. The system must be able to match the identity of the portal user to the identity of the same user in the agency system.**
☒ P, Q, N or I Notes: P	**15. Single sign-on. The system must support single sign-on to the agency application.**
☒ P, Q, N or I Notes: I – state yes but reply is a restating of the requirement	**16. Import user profile data from agency systems. The system must be able to import user data from different SoM applications to ensure offboarding happens in a timely manner, so that government resources are protected from fraud. (example: death records)**
☒ P, Q, N or I Notes: P	**17. History logging.** 1) The system must log all actions taken by:
	a) Constituents
	b) MaineIT support
	Including but not limited to:

	c) who made the change
	d) when the change was made
	e) what changed
☒ P, Q, N or I Notes: Y	**18. Reporting. The logging data (history) must be available for constituent and system dashboards and reporting in general.**
☒ P, Q, N or I Notes: Y	**19. Security Controls. The system must comply to the following security controls:**
	1) DDOS Protections[WN1] ,
	2) OWASP Top 10
	a) Cross Site Scripting,
	b) SQL Injection,
	3) Authentication bypass,
	a) poorly authenticated APIs,
	b) Role based access controls,
	c) proper session control
	4) Real-time visibility,
	5) Anomalous behavior,
	6) User sign with geo-location tracking,
	Geo-blocking capabilities.
	Security controls must include Web Application Firewall [WN1]
☒ P, Q, N or I Notes: Q – does this meet the requirement, for 1)?	**20. General System Requirements.** 1) Mobile Support with Native App; (iOS and Android)
	2) System availability: 24/7 with 4x1-hour outages per year
	3) Identity relationships must be tracked in the cloud infrastructure.
	4) Support responsive web and web browsers.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Microsoft
DATE: 6/3/2-24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

	a. Supports Windows, Chrome, and Macintosh operating systems
☒ P, Q, N or I Notes: P – basic, yes will address during discovery.	**21. Training and Support.** 1) Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
	2) MaineIT will require technical/administrator training. There will be initial training and on-going training as users are added.
	3) Have a continuous process to ensure constituents that may have run into issues setting up accounts can have help 24/7.
☒ P, Q, N or I Notes: P – basic, yes will address during discovery.	**22. Support Requirements** 1) The Bidder will provide support, and maintenance for the solution to begin immediately after receiving the State's official acceptance of the implemented solution.
	2) Support and maintenance will be provided for the terms and duration specified in the contract.
	3) The Bidder will address all questions and reported problems related to the technical and functional operation of the system.
	4) The Bidder must provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours: 8:00 a.m. to 5:00 p.m. Eastern Standard Time.
	5) As part of the maintenance agreement, the Bidder will make all product releases and upgrades available to the State at no additional charge.
	6) All release and upgrades shall be implemented and tested by the Bidder, outside of the normal operating hours of the State government.
	7) User testing shall occur during normal State business hours. All remediation of failed testing cases and protocols shall also

	occur outside of the normal operating hours of the State government.
☒ P, Q, N or I Notes: I - After reviewing most of the security requirements and policies, the expectation is the system will comply without waivers.	**23. Hosting** Solution can comply with MaineIT remote hosting policies. a) Remote Hosting Policy http://maine.gov/oit/policies/RemoteHostingPolicy.pdf b) Hosting Customization Policy http://maine.gov/oit/policies/HostingCustomizationPolicy.pdf
☒ P, Q, N or I Notes: P	**24. Disaster Recovery** Proposed Solution can comply with MaineIT security requirements and remote hosting requirements, without requiring waivers, before contract finalization.
	1) Maintaining an availability metric of ninety-nine-point nine percent (99.9%) of uptime
	2) Ensuring the capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six hours (i.e., maximum data loss cannot exceed six (6) hours);
	3) Ensuring a recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours;
	4) Ensuring the hosting environment provides adequate capacity to ensure that, under ethernet connectivity to the client device, data inquiry/lookup response is within three (3) seconds, and data modification response is within five (5) seconds;
	5) Providing the Department at least thirty (30) calendar day advance written notice of any material change in network operations or architecture;

	6) Ensuring any planned material change in network operations or architecture cannot be made without the prior written consent of the Department; and Outlining of all Service Level Agreements (SLAs) for technical support (the awarded Bidder shall be open to negotiation to ensure the SLAs meet the Department's needs

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

☒1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.

P, N, Q, or I & Notes: I – I do not think MS has an understanding of what we have asked for based on this sentence: To resolve this issue, we understand that Maine is seeking an overall approach to translate those non-emergency public-facing services into true digitally enabled services. Pg. 2

☒1b) Detailed description of the technologies, software and / or hardware for each of the components.

P, N, Q, or I & Notes: P – although many read like marketing material.

☒1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.

P, N, Q, or I & Notes: N – did not state why it is best for the state and comes across as marketing jargon.

☒1d) Description of the overall platform and architecture of the proposed solution(s).

P, N, Q, or I & Notes: P – but schematic is overly complicated, pg. 11

☒1e) Description of any third-party software or partnerships required for the proposed Solution(s).

P, N, Q, or I & Notes: P

☒2a) A detailed timeline and description of milestones, deliverables, tasks
P, N, Q, or I & Notes: N – a detailed timeline will be developed during program planning.

☒2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period
P, N, Q, or I & Notes: P

☒2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
P, N, Q, or I & Notes: N – same as 2a above.

☒2d) Average time to market for each component.
P, N, Q, or I & Notes: N – same as 2a above.

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. ☒Capture Constituent Identity and profile data.
   P, N, Q, or I & Notes:
b. ☒Provide identity provisioning and deprovisioning.
   P, N, Q, or I & Notes:
c. ☐Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
   i. Identity Creation
   ii. Identity provisioning
   iii. Attribute maps
   iv. Authentication (e.g., password policies and synchronization)
      P, N, Q, or I & Notes: P

d. ☒Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies.
   P, N, Q, or I & Notes:

e. ☒Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
   P, N, Q, or I & Notes: I – The solution will be able to integrate with up to 5 agencies as part of the initial implementation.

f. ☐Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.
   P, N, Q, or I & Notes: N – did not address this

g. ☐Allow for multiple role selections for the following identities:
   i. Individual
   ii. Business Owner
   iii. Support multiple identities for State employees that work with the portal in a support role:
      (a) SOM Employee identity and credentials for supporting the application.
      (b) Constituent identity and credentials to use the state services offered through the portal.
   iv. Multi role individual (Individual and Business Owner)
      P, N, Q, or I & Notes: N – Did not address this

h. ☐Have the ability to provide levels of proofing which will be directly tied to the Constituent's level of consent given.
   P, N, Q, or I & Notes: N – did not address this

i. ☒Support multi-factor authentication to protect against user impersonation and credential theft.
   P, N, Q, or I & Notes: P

B.2. ☐The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.

P, N, Q, or I & Notes: P – pg 38

a. Disclosure and Consent Management

The desire of the State is to be as transparent as possible and respect the privacy of the individual interacting with the Constituents' Portal. Consent is a core tenant of maintaining the public trust in the Constituents' Portal and will be a foundational component of the architecture.

The Disclosure and Consent Management solution shall include:

i. ☒Granular consent management that encompasses the automated functions necessary to create, modify, revoke, and manage Constituent consents.
ii. ☒Allow users the ability to opt-in and opt-out of data sharing and services within the Constituents' portal.
iii. ☒Obtain user consent both in an interactive and set preference mode for a variety of transactions on the Portal.
iv. ☒Support administrative users' management of standard legal disclaimers and data classification for transactions.
v. ☒Highly configurable with version control and history tracking for consent language. N – did not address
vi. ☒Ability for end user to access a retrievable log of granted consent and data usage on the portal derived from the consent. N – did not address

P, N, Q, or I & Notes: N – did not address all

b. Recommendation Technology

The State is seeking options which, while maintaining individual privacy, will collect and analyze data about user interactions, behavior, and preferences. The expected outcome of this will be to provide insights and intelligence that help the State make informed decisions and improve Constituent experiences.

i. ☐From the user perspective, the portal should be able to make real-time recommendations for related services.
ii. ☐Data captured in this environment must be obfuscated, as to not allow any party to directly target or track the preferences of an individual or their usage of the portal.
iii. ☐Solution providers should discuss in detail their use, storage, destruction of metadata, and tracking technologies with emphasis on how their offering provides analytical insights while protecting the individual user privacy.

P, N, Q, or I & Notes: N – did not address but said could be aligned during development. The accuracy of model results will be co-discussed and aligned during the development. We will decide on the best performance solution based on criteria of accuracy, cost saving and consistency.

c. Data Management

The State is seeking the ability for the portal's Constituent identity to be linked to records maintained by individual State agencies. The proposed solution will include:

- i. ☐Capabilities to streamline the sharing of data between State systems, including
  - i. The identity assurance level
  - ii. Agency to user notifications
  - iii. Verification of user consent
  - iv. Identity resolution
  - v. Data sharing between agencies.
- ii. ☒Maintain a central repository of basic (core) Constituent data, that can be used by any State application to reduce data redundancy, and outdated or inaccurate information while maintaining confidentiality.
- iii. ☒Ability to integrate with State applications using, OpenID, OAuth, Web Services Federation Protocol (WS-Fed), Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), Active Directory, Application Programming Interface (API) or equivalent protocols.
  - (a) ☐Ability to match the identity of the portal user to the identity of the same user in the Agency system. N – did not address
- iv.
- v. ☐Log all actions taken by:
  - i. Constituents
  - ii. MaineIT Support, including:
    - (a) Who made the change
    - (b) When the change was made
    - (c) What changed to and from N – did not address
    - (d) ☐Logging data must be available for system dashboards and reporting. N – did not address
- vi.

  - (a) P, N, Q, or I & Notes: N – did not address

d. Customer Service
The State is seeking solution(s) to provide 24/7/365 customer service to Constituents regardless of their location or technical abilities.
  i. ☒Support Constituents with personalized and timely assistance.
  ii. ☒Provide the state options to support our Constituents across multiple channels including, but not limited to phone, email, chat, etc.

P, N, Q, or I & Notes: N – did not address phone support, virtual agent instead. Our solution has the ability to integrate with the state's existing centralized service desk, as applicable, to address those rate situations where direct human interaction is necessary.

C.1. General System
a. ☒Mobile support with native app (iOS and Android)
b. ☒System availability: 24/7 with a maximum of four (4) 1-hour outages per year
c. ☒Identity relationships must be tracked in the cloud infrastructure.
d. ☒Support responsive web and web browsers.
  i. ☒Supports Windows, Chrome, and Macintosh operating systems.

P, N, Q, or I & Notes: P

C.2. ☒Compliance with MaineIT Policies & Standards
a. Architecture Compliance Policy
b. System and Services Acquisition Policy and Procedures (SA-1)
c. Application Deployment Certification Policy
d. Digital Accessibility Policy
e. Remote Hosting Policy
f. Data Exchange Policy
g. Information Security Policy
h. Access Control Policy (AC-1)
i. Access Control Procedures for Users (AC-2)
j. Risk Assessment Policy and Procedures (RA-1)
k. Vulnerability Scanning Procedure (RA-5)
l. Security Assessment and Authorization Policy and Procedures (CA-1)
m. System and Information Integrity Policy and Procedures (SI-1)
n. Configuration Management Policy (CM-1)

o. Web Standards

P, N, Q, or I & Notes: N – did not address adhere to all policies and stated "many." Instead, with lacking detail.

C.3. Support and Maintenance

a. ☒Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State's official acceptance of the implemented solution.
P, N, Q, or I & Notes: N – did not respond
b. ☐Terms and duration of the support and maintenance will be specified in the contract.
P, N, Q, or I & Notes:

c. ☐All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
P, N, Q, or I & Notes:
d. ☐Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
P, N, Q, or I & Notes:
e. ☐All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
P, N, Q, or I & Notes:
f. ☐All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
P, N, Q, or I & Notes:
g. ☐User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
P, N, Q, or I & Notes:

N – overall this whole area was not addressed specifically.

4. Security

The proposed solutions must provide a robust security system that aligns with the States Security Policies, standards, and Processes, Including:

Comply with or have the following security certifications:

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Microsoft
DATE: 6/3/2-24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

i. ☐National Institute of Standards and Technology (NIST) 800-53
ii. ☐FedRamp
iii. ☐Health Insurance Portability and Accountability Act (HIPAA)
iv. ☐SOC 2 Type II
v. ☐Comply to the following security controls:
vi. ☐DDOS Protections [WN1]
vii. ☐Open Web Application Security Project (OWASP) Top 10
viii. ☐Cross Site Scripting
ix. ☐Structured Query Language (SQL) Injection
x. ☐Authentication bypass
xi. ☐Poorly authenticated APIs
xii. ☐Role based access controls
xiii. ☐Proper session control
xiv. ☐Real-time visibility
xv. ☐Anomalous behavior
xvi. ☐User sign with geo-location tracking
xvii. ☐Geo-blocking capabilities.
xviii. ☐Web Application Firewall [WN1]
xix. ☐System security must include the following security components:
xx. ☐Account take over protections
xxi. ☐Account sign-in Protections
xxii. ☐Behavior detection and evaluation
xxiii. ☐Adaptive AI Technology
xxiv. ☐Bot Protection; identity visitor behavior through analysis, technical and behavioral data.
xxv. ☐The proposed solution must be able to integrate with the State Security Information and Event Monitoring (SIEM) Splunk. Ability to log security information and events.

P, N, Q, or I & Notes: I – did not specifically address SoM polices, standards, etc.

5. Licensing

☒The State is aware that multiple licensing options are available and will be required to support the proposed solution in its entirety. The State seeks bids which will provide the most cost-effective licensing approach. Bidders are required to provide a detail breakdown for the proposed licensing.

P, N, Q, or I & Notes: I – detail not very understandable.

1. **Training and OCM (Organizational Change Management)**
   a. ☒Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
   b. ☒Training must include technical and administrator training, initial and ongoing as users are added.
   c. ☐Continuous process to ensure Constituents that may have run into issues setting up accounts have help 24/7. N – did not address this one
   d. ☒Bidders shall guide the State in OCM engagement for the duration of project planning, transition, and final implementation phase including:
      i. Designing and managing team structures with roles and responsibilities to facilitate automated program delivery, while noting any risks anticipated from the lack of readiness in the organization and staffing.
      ii. Ensure a successful transition for the integration of new processes and technology with stakeholders.
      iii. Organizational readiness assessment N – did not address this one

P, N, Q, or I & Notes: N – overall Neg on this section.

3. **Disaster Recovery**
   a. ☒Availability of ninety-nine-point nine percent (99.9%) of uptime
   b. ☒Capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six (6) hours (i.e., maximum data loss cannot exceed six (6) hours)
   c. ☒Recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours.

P, N, Q, or I & Notes: P

4. **Feature Enhancements**

a. ☒The State is seeking two hundred and fifty (250) hours of time and material for each proposed technology (CIAM), Personalized Dashboard, Disclosure and Consent Management, Data Management, and Recommendation Technology) to allow for specifications and enhancements during the contract period.

P, N, Q, or I & Notes: P

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Microsoft
DATE: 6/3/2-24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

5. Project Management

a. ☒The State plans to have its own project manager however, the awarded Bidder must have a project manager that has the primary responsibility for executing the project management tasks associated with the project. The awarded Bidder will:
   i. Work in collaboration with the State's Project Manager
   ii. Align with State Project Management processes and practices.

b. ☐Manage the implementation, executing all activities, tasks, deliverables and resource needs, both state and awarded Bidder.

c. ☐Track project status including managing and tracking all project risks, issues and decisions.

d. ☐Track and report status of deliverables and project status

e. ☐The awarded Bidder will provide their approach for project management and administration services including:
   i. Project Management Methodology
   ii. Project Governance
   iii. Resource Allocation and Schedule Management approach
   iv. Communication Management Approach including status reporting and document repository management.
   v. Risk and Issue Management Methodology
   vi. Change Management Methodology
   vii. Quality Management Methodology

   P, N, Q, or I & Notes: N – bidder did not address nearly any of these requirements in this section. Pg.58

D. Value Added Options (Other)

☒Bidders shall provide value added optional services to address relevant matters that have not been anticipated in this RFP but contribute to successful implementation of the proposed solutions, as well as any technology or services that will reduce risk to the project's quality and continuity. The value-added technology and services will not be included in the evaluation process but may be added during the contract negotiations.

P, N, Q, or I & Notes: P

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: PruTech
DATE: 6/7/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

Section I – Preliminary Information (No points – Eligibility Requirements)

(File #1 App. A, B, C)
☒Done – Pass/Fail by Procurement & RFP Coordinator

Section II Organization Qualifications and Experience

(File #2 – App. D, E + other areas that have no Appendix number but are part of File #2)

1. **Overview of the Organization (App. D)**
   ☒Bidders must include three examples of projects which demonstrate their experience and expertise in performing these services as well as highlighting the Bidder's stated qualifications and skills.

   Statement of qualifications
   ☒Client name, contact person, Ph#, email.
   Contract history with the state may be considered in rating proposals even if not provided by the bidder.

   P, N, Q, or **I** & Notes:

6 projects, all covering various different components of our requirements; no single project fullfill all

2. **Subcontractors (App. E)**
   ☒If subcontractors are to be used, Bidders must provide the name, address, phone number, contact person, and a brief description of the subcontractors' organizational capacity and qualifications.
   Business name, contact person, address, ph#, email.
   P, N, Q, or I & Notes:

3. **Organizational Chart (No Appendix)**
   ☒Bidders must provide an organizational chart. The organizational chart must include the project being proposed. Each position must be identified by position title and corresponding to the personnel job descriptions.
   P, N, Q, or I & Notes:

4. **Litigation (No App.)**

☐Bidders must attach a list of all current litigation in which the Bidder is named and a list of all closed cases that have closed within the past five (5) years in which the Bidder paid the claimant either as part of a settlement or by decree. For each, list the entity bringing suit, the complaint, the accusation, amount, and outcome.
P, N, Q, or **I** & Notes:

5. **Financial Viability (No App.)**
☐Bidders must provide a current copy of their Dun & Bradstreet Business Information Report Snapshot.
P, N, Q, or **I** - Notes:

6. **Licensure/Certification (No App.)**
☐Bidders *may* provide documentation of any applicable licensure/certification or specific credentials that are related to providing the proposed services of the RFP.
P, N, Q, or **I** & Notes:
Certificate for iso 9001:2015

7. **Certificate of Insurance (No App.)**
☒Bidders must provide a certificate of insurance on a standard ACORD form (or the equivalent) evidencing the Bidder's general liability, professional liability and any other relevant liability insurance policies that might be associated with the proposed services.
P, N, Q, or **I** & Notes:

Section III - Proposed Services

(File #3 – App. F, G, H)

1. **Technical Assessment (App. F)**
☒Done

2. **Services to be Provided (App. G)**

Note: on App. G Detailed Technical and Functional Requirements Excel spreadsheet, a tab is labeled User Stories. No response is required for Tab 3; these were provided to bidders for clarity and understanding of the expected journey a Constituent will experience.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: PruTech
DATE: 6/7/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

☒ **P**, Q, N or I Notes: Detailed replies to tactical how account take over and sign in protections work	**1. System security components System security must include the following security components:**
	1) Account Take Over Protections
	a) Account Sign-in Protections
	a) Account Sign-in Protections
	a) Adaptive AI Technology
	b) Bot Protection: identify visitor behavior through analysis of technical and behavioral data.
☒ P, Q, N or **I** Notes: Mention of tier vs level as well as needing hardware for inperson document	**2. Identity Proofing must have the ability to provide levels of proofing which will be directly tied to the constituent's level of access.**
	1) Define various levels of id proofing
	2) Document Image Capture
	3) Close coupling with authentication
☒ **P**, Q, N or I Notes:	**3. Multi-factor authentication The system must support multi-factor authentication to protect against user impersonation and credential theft.**
☒ **P**, Q, N or I Notes:	**4. Risk-based factors The system must support risk-based factors and scores that are based on factors such as, but not limited to, device and location.**
☐ P, Q, N or **I** Notes:	**5. Identity lifecycle management components The system must include the following identity lifecycle management components for risk-based critical applications not limited to end users but also for generic accounts and system/service accounts:**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: PruTech
DATE: 6/7/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

No mention of which sources it can ingest	1) Identity Creation
	2) Identity provisioning
	3) Attribute maps
	4) Authentication (e.g., password policies and synchronization)

☒ **P**, Q, N or I Notes:	**6. Security event logging The system must log security information and events.**
	Security Information and Event Management (SIEM) – Splunk
	Cloud Services: Azure, AWS, Oracle, Google
☒ P, Q, N or **I** Notes:	**7. Security Certifications The system must comply too or have the following security certifications:**
No mention of HIPAA for okta or thales	1) NIST 800-53
	2) FedRamp
	3) HIPAA
	4) SOC 2 Type II
	Note:
	IRS require a 45-day letter approval for new cloud solutions.
☒ P, Q, N or **I** Notes: no mention of thales logs?	**8. SIEM (Splunk) integration The system must be able to integrate with the State of Maine Security Information and Event Monitoring (SIEM) Splunk for Security Operations Center operations.**
☒ **P**, Q, N or I Notes:	**9. Core constituent data. The system must maintain a central repository of basic (core) constituent data, that can be used by any SoM application to reduce**

	data redundancy and outdated or inaccurate information while maintaining confidentiality.
☒ P, Q, N or **I** Notes:	**11. Data Management. The system must apply the Data Management Rules to the constituent profile data as per the SoM Data Management Policies.**
☒ P, Q, N or **I** Notes:	**12. SOM Employee. The system must support multiple identities for SOM employees that work with the portal in a support role.**
Possible with different accounts/personas no details on the how	1) SOM Employee identity and credentials for supporting the application.
	2) Constituent identity and credentials to use the state services offered through the portal.

☒ P, Q, N or **I** Notes:	**13. APIs. The system must be able to connect to at least one agency application.**
	Considerations:
	a) OpenID, OAuth, WS-Fed, SAML, LDAP, Active Directory, Application Programming Interfaces (APIs), Software Development
	b) Develop once and reuse often with other agencies would be ideal
☒ P, **Q**, N or I Notes: how does it hand dubs or matches without appending the 1	**14. User identification matching. The system must be able to match the identity of the portal user to the identity of the same user in the agency system.**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: PruTech
DATE: 6/7/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

☒ **P**, Q, N or I Notes:	**15. Single sign-on. The system must support single sign-on to the agency application.**
☒ P, Q, N or **I** Notes: How does this work with question 14	**16. Import user profile data from agency systems. The system must be able to import user data from different SoM applications to ensure offboarding happens in a timely manner, so that government resources are protected from fraud. (example: death records)**
☒ P, Q, N or **I** Notes:	**17. History logging.** 1) The system must log all actions taken by:
Does "solution" mean both okta and thales	a) Constituents
	b) MaineIT support
	Including but not limited to:
	c) who made the change
	d) when the change was made
	e) what changed
☒ P, Q, **N** or I Notes: does not call out reporting back to constituent	**18. Reporting. The logging data (history) must be available for constituent and system dashboards and reporting in general.**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: PruTech
DATE: 6/7/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, **N** or I Notes:	**19. Security Controls. The system must comply to the following security controls:**
	1) DDOS Protections[WN1] ,
	2) OWASP Top 10
What about thales?	a) Cross Site Scripting,
	b) SQL Injection,
	3) Authentication bypass,
	a) poorly authenticated APIs,
	b) Role based access controls,
	c) proper session control
	4) Real-time visibility,
	5) Anomalous behavior,
	6) User sign with geo-location tracking,
	Geo-blocking capabilities.
	Security controls must include Web Application Firewall [WN1]
☒ P, Q, N or **I** Notes:	**20. General System Requirements.** 1) Mobile Support with Native App; (iOS and Android)
Not fully met	2) System availability: 24/7 with 4x1-hour outages per year
	3) Identity relationships must be tracked in the cloud infrastructure.
	4) Support responsive web and web browsers.
	a. Supports Windows, Chrome, and Macintosh operating systems
☒ P, Q, N or **I** Notes:	**21. Training and Support.** 1) Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.

	2) MaineIT will require technical/administrator training. There will be initial training and on-going training as users are added.
	3) Have a continuous process to ensure constituents that may have run into issues setting up accounts can have help 24/7.
☒ P, Q, N or **I** Notes:	**22. Support Requirements** 1) The Bidder will provide support, and maintenance for the solution to begin immediately after receiving the State's official acceptance of the implemented solution.
Is this adjustable	2) Support and maintenance will be provided for the terms and duration specified in the contract.
	3) The Bidder will address all questions and reported problems related to the technical and functional operation of the system.
Does not specify toll free	4) The Bidder must provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours: 8:00 a.m. to 5:00 p.m. Eastern Standard Time.
	5) As part of the maintenance agreement, the Bidder will make all product releases and upgrades available to the State at no additional charge.
	6) All release and upgrades shall be implemented and tested by the Bidder, outside of the normal operating hours of the State government.
	7) User testing shall occur during normal State business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State government.
☐ P, Q, **N** or I Notes: B) missing thales info	**23. Hosting** Solution can comply with MaineIT remote hosting policies. a) Remote Hosting Policy http://maine.gov/oit/policies/RemoteHostingPolicy.pdf b) Hosting Customization Policy http://maine.gov/oit/policies/HostingCustomizationPolicy.pdf
☐ P, Q, **N** or I Notes:	**24. Disaster Recovery** Proposed Solution can comply with MaineIT security requirements and remote hosting requirements, without requiring waivers, before contract finalization.
Does not incudled	1) Maintaining an availability metric of ninety-nine-point nine percent (99.9%) of uptime

thales uptime; does not meet rto	
	2) Ensuring the capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six hours (i.e., maximum data loss cannot exceed six (6) hours);
	3) Ensuring a recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours;
	4) Ensuring the hosting environment provides adequate capacity to ensure that, under ethernet connectivity to the client device, data inquiry/lookup response is within three (3) seconds, and data modification response is within five (5) seconds;
	5) Providing the Department at least thirty (30) calendar day advance written notice of any material change in network operations or architecture;
	6) Ensuring any planned material change in network operations or architecture cannot be made without the prior written consent of the Department; and Outlining of all Service Level Agreements (SLAs) for technical support (the awarded Bidder shall be open to negotiation to ensure the SLAs meet the Department's needs

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

☒1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
P, N, Q, or **I** & Notes:

☒1b) Detailed description of the technologies, software and / or hardware for each of the components.
P, N, Q, or **I** & Notes:

☒1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.

P, N, Q, or I & Notes:

☒1d) Description of the overall platform and architecture of the proposed solution(s).
P, N, Q, or **I** & Notes:
Missing true architectural diagram

☒1e) Description of any third-party software or partnerships required for the proposed Solution(s).
P, N, Q, or I & Notes:
Good calls for both software and subcontractors

☒2a) A detailed timeline and description of milestones, deliverables, tasks
P, N, Q, or **I** & Notes:
Lacking deliverables

☒2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period
P, N, Q, or I & Notes:

☐2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
P, N, Q, or I & Notes:

☐2d) Average time to market for each component.
P, N, Q, or I & Notes:

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. ☒Capture Constituent Identity and profile data.

P, N, Q, or I & Notes:

b. ☒Provide identity provisioning and deprovisioning.
P, N, Q, or I & Notes:

c. ☒Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
   i. Identity Creation
   ii. Identity provisioning
   iii. Attribute maps
   iv. Authentication (e.g., password policies and synchronization)
      P, N, Q, or I & Notes:

d. ☒Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies.
P, N, Q, or **I** & Notes:
Mention of ID proof happing with okta as well as thales

e. ☒Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
P, N, Q, or I & Notes:

f. ☒Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.
P, N, Q, or **I** & Notes:

g. ☐Allow for multiple role selections for the following identities:
   i. Individual
   ii. Business Owner
   iii. Support multiple identities for State employees that work with the portal in a support role:
      (a) SOM Employee identity and credentials for supporting the application.
      (b) Constituent identity and credentials to use the state services offered through the portal.
   iv. Multi role individual (Individual and Business Owner)
      P, **N**, Q, or I & Notes:
      Does really talk to the uses cases mentioned above

h. ☒Have the ability to provide levels of proofing which will be directly tied to the Constituent's level of consent given.
P, **N**, Q, or I & Notes: does not talk to the question or how okta thales work together

i. ☒Support multi-factor authentication to protect against user impersonation and credential theft.
P, N, Q, or I & Notes:

B.2. ☒The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.
P, N, Q, or **I** & Notes:

a. Disclosure and Consent Management

The desire of the State is to be as transparent as possible and respect the privacy of the individual interacting with the Constituents' Portal. Consent is a core tenant of maintaining the public trust in the Constituents' Portal and will be a foundational component of the architecture.

The Disclosure and Consent Management solution shall include:

i. ☒Granular consent management that encompasses the automated functions necessary to create, modify, revoke, and manage Constituent consents.
ii. ☒Allow users the ability to opt-in and opt-out of data sharing and services within the Constituents' portal.
iii. ☒Obtain user consent both in an interactive and set preference mode for a variety of transactions on the Portal.
iv. ☒Support administrative users' management of standard legal disclaimers and data classification for transactions.
v. ☒Highly configurable with version control and history tracking for consent language.
vi. ☒Ability for end user to access a retrievable log of granted consent and data usage on the portal derived from the consent.

P, **N**, Q, or I & Notes: no detail on how it works

b. Recommendation Technology

The State is seeking options which, while maintaining individual privacy, will collect and analyze data about user interactions, behavior, and preferences. The expected outcome of this will be to provide insights and intelligence that help the State make informed decisions and improve Constituent experiences.

i. ☒From the user perspective, the portal should be able to make real-time recommendations for related services.
ii. ☒Data captured in this environment must be obfuscated, as to not allow any party to directly target or track the preferences of an individual or their usage of the portal.
iii. ☒Solution providers should discuss in detail their use, storage, destruction of metadata, and tracking technologies with emphasis on how their offering provides analytical insights while protecting the individual user privacy.

P, N, Q, or **I** & Notes:

c. Data Management

The State is seeking the ability for the portal's Constituent identity to be linked to records maintained by individual State agencies. The proposed solution will include:

i. ☒Capabilities to streamline the sharing of data between State systems, including
    i. The identity assurance level
    ii. Agency to user notifications
    iii. Verification of user consent
    iv. Identity resolution
    v. Data sharing between agencies.
ii. ☒Maintain a central repository of basic (core) Constituent data, that can be used by any State application to reduce data redundancy, and outdated or inaccurate information while maintaining confidentiality.
iii. ☒Ability to integrate with State applications using, OpenID, OAuth, Web Services Federation Protocol (WS-Fed), Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), Active Directory, Application Programming Interface (API) or equivalent protocols.
iv. ☒Ability to match the identity of the portal user to the identity of the same user in the Agency system.
v. ☒Log all actions taken by:

    i. Constituents
    ii. MaineIT Support, including:
        (a) Who made the change
        (b) When the change was made
        (c) What changed to and from
  vi. ☒Logging data must be available for system dashboards and reporting.

P, N, Q, or **I** & Notes:
Mentions aws; but does not list that as a product set

d. Customer Service

The State is seeking solution(s) to provide 24/7/365 customer service to Constituents regardless of their location or technical abilities.

  i. ☒Support Constituents with personalized and timely assistance.
  ii. ☒Provide the state options to support our Constituents across multiple channels including, but not limited to phone, email, chat, etc.

P, N, Q, or I & Notes:
Provided by cybolt

C.1. General System

  a. ☐Mobile support with native app (iOS and Android)
  b. ☐System availability: 24/7 with a maximum of four (4) 1-hour outages per year
  c. ☒Identity relationships must be tracked in the cloud infrastructure.
  d. ☒Support responsive web and web browsers.
    i. ☒Supports Windows, Chrome, and Macintosh operating systems.

P, **N**, Q, or I & Notes:
No mention of thales uptime; no native app – web based

C.2. ☒Compliance with MaineIT Policies & Standards

  a. Architecture Compliance Policy
  b. System and Services Acquisition Policy and Procedures (SA-1)
  c. Application Deployment Certification Policy
  d. Digital Accessibility Policy
  e. Remote Hosting Policy
  f. Data Exchange Policy
  g. Information Security Policy

h. Access Control Policy (AC-1)
i. Access Control Procedures for Users (AC-2)
j. Risk Assessment Policy and Procedures (RA-1)
k. Vulnerability Scanning Procedure (RA-5)
l. Security Assessment and Authorization Policy and Procedures (CA-1)
m. System and Information Integrity Policy and Procedures (SI-1)
n. Configuration Management Policy (CM-1)
o. Web Standards

P, N, Q, or **I** & Notes:

C.3. Support and Maintenance

a. ☒Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State's official acceptance of the implemented solution.
   P, **N**, Q, or I & Notes: no support detail
b. ☒Terms and duration of the support and maintenance will be specified in the contract.
   P, **N**, Q, or I & Notes: no supporting detail

c. ☒All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
   P, **N**, Q, or I & Notes: no supporting detail
d. ☒Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
   P, **N**, Q, or I & Notes: no supporting detail; was mentioned cybolt was for support
e. ☒All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
   P, N, Q, or **I** & Notes:
f. ☒All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
   P, **N**, Q, or I & Notes: no supporting detail
g. ☒User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.

P, **N**, Q, or I & Notes: no support detail

4. Security

The proposed solutions must provide a robust security system that aligns with the States Security Policies, standards, and Processes, Including:

Comply with or have the following security certifications:

i. ☐National Institute of Standards and Technology (NIST) 800-53
ii. ☐FedRamp
iii. ☐Health Insurance Portability and Accountability Act (HIPAA)
iv. ☐SOC 2 Type II
v. ☐Comply to the following security controls:
vi. ☐DDOS Protections [WN1]
vii. ☐Open Web Application Security Project (OWASP) Top 10
viii. ☐Cross Site Scripting
ix. ☐Structured Query Language (SQL) Injection
x. ☐Authentication bypass
xi. ☐Poorly authenticated APIs
xii. ☐Role based access controls
xiii. ☐Proper session control
xiv. ☐Real-time visibility
xv. ☐Anomalous behavior
xvi. ☐User sign with geo-location tracking
xvii. ☐Geo-blocking capabilities.
xviii. ☐Web Application Firewall [WN1]
xix. ☐System security must include the following security components:
xx. ☐Account take over protections
xxi. ☐Account sign-in Protections
xxii. ☐Behavior detection and evaluation
xxiii. ☐Adaptive AI Technology
xxiv. ☐Bot Protection; identity visitor behavior through analysis, technical and behavioral data.
xxv. ☐The proposed solution must be able to integrate with the State Security Information and Event Monitoring (SIEM) Splunk. Ability to log security information and events.

P, **N**, Q, or **I** & Notes: no mention of thales for idproof or purtech for dashboarding

5. Licensing

☐The State is aware that multiple licensing options are available and will be required to support the proposed solution in its entirety. The State seeks bids which will provide the most cost-effective licensing approach. Bidders are required to provide a detail breakdown for the proposed licensing.

P, **N**, Q, or **I** & Notes:
Missing licensing attachment

1. Training and OCM (Organizational Change Management)

a. ☒Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
b. ☒Training must include technical and administrator training, initial and ongoing as users are added.
c. ☐Continuous process to ensure Constituents that may have run into issues setting up accounts have help 24/7.
d. ☐Bidders shall guide the State in OCM engagement for the duration of project planning, transition, and final implementation phase including:
   i. Designing and managing team structures with roles and responsibilities to facilitate automated program delivery, while noting any risks anticipated from the lack of readiness in the organization and staffing.
   ii. Ensure a successful transition for the integration of new processes and technology with stakeholders.
   iii. Organizational readiness assessment

P, N, Q, or **I** & Notes:
Nothing reference 24/7

3. Disaster Recovery

a. ☐Availability of ninety-nine-point nine percent (99.9%) of uptime
b. ☐Capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six (6) hours (i.e., maximum data loss cannot exceed six (6) hours)
c. ☐Recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours.

P, **N**, Q, or I & Notes:
Nothing about thales or prutech dr

4. Feature Enhancements

a. ☒The State is seeking two hundred and fifty (250) hours of time and material for each proposed technology (CIAM), Personalized Dashboard, Disclosure and Consent Management, Data Management, and Recommendation Technology) to allow for specifications and enhancements during the contract period.

P, N, Q, or I & Notes:

5. Project Management

a. ☒The State plans to have its own project manager however, the awarded Bidder must have a project manager that has the primary responsibility for executing the project management tasks associated with the project. The awarded Bidder will:
    i. Work in collaboration with the State's Project Manager
    ii. Align with State Project Management processes and practices.
b. ☒Manage the implementation, executing all activities, tasks, deliverables and resource needs, both state and awarded Bidder.
c. ☒Track project status including managing and tracking all project risks, issues and decisions.
d. ☒Track and report status of deliverables and project status
e. ☒The awarded Bidder will provide their approach for project management and administration services including:
    i. Project Management Methodology
    ii. Project Governance
    iii. Resource Allocation and Schedule Management approach
    iv. Communication Management Approach including status reporting and document repository management.
    v. Risk and Issue Management Methodology
    vi. Change Management Methodology
    vii. Quality Management Methodology

P, N, Q, or **I** & Notes:

D. Value Added Options (Other)

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: PruTech
DATE: 6/7/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

☒Bidders shall provide value added optional services to address relevant matters that have not been anticipated in this RFP but contribute to successful implementation of the proposed solutions, as well as any technology or services that will reduce risk to the project's quality and continuity. The value-added technology and services will not be included in the evaluation process but may be added during the contract negotiations.

P, N, Q, or **I** & Notes:

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: PruTech
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

Section I – Preliminary Information (No points – Eligibility Requirements)

(File #1 App. A, B, C)

☒Done – Pass/Fail by Procurement & RFP Coordinator

Section II Organization Qualifications and Experience

(File #2 – App. D, E + other areas that have no Appendix number but are part of File #2)

1. Overview of the Organization (App. D)

☒Bidders must include three examples of projects which demonstrate their experience and expertise in performing these services as well as highlighting the Bidder's stated qualifications and skills.

Statement of qualifications

☒Client name, contact person, Ph#, email.

Contract history with the state may be considered in rating proposals even if not provided by the bidder.

P, N, Q, or I & Notes:P

2. Subcontractors (App. E)

☒If subcontractors are to be used, Bidders must provide the name, address, phone number, contact person, and a brief description of the subcontractors' organizational capacity and qualifications.

Business name, contact person, address, ph#, email.

P, N, Q, or I & Notes:P

3. Organizational Chart (No Appendix)

☒Bidders must provide an organizational chart. The organizational chart must include the project being proposed. Each position must be identified by position title and corresponding to the personnel job descriptions.

P, N, Q, or I & Notes:P

4. Litigation (No App.)

☒Bidders must attach a list of all current litigation in which the Bidder is named and a list of all closed cases that have closed within the past five (5) years in which the Bidder paid the claimant either as part of a settlement or by decree. For each, list the entity bringing suit, the complaint, the accusation, amount, and outcome.
P, N, Q, or I & Notes:Q 3 years instead of 5 years attached letter says 5

5. **Financial Viability (No App.)**
☒Bidders must provide a current copy of their Dun & Bradstreet Business Information Report Snapshot.
P, N, Q, or I - Notes:P

6. **Licensure/Certification (No App.)**
☒Bidders *may* provide documentation of any applicable licensure/certification or specific credentials that are related to providing the proposed services of the RFP.
P, N, Q, or I & Notes:P

7. **Certificate of Insurance (No App.)**
☒Bidders must provide a certificate of insurance on a standard ACORD form (or the equivalent) evidencing the Bidder's general liability, professional liability and any other relevant liability insurance policies that might be associated with the proposed services.
P, N, Q, or I & Notes:P

Section III - Proposed Services
(File #3 – App. F, G, H)

1. **Technical Assessment (App. F)**
☒Done

2. **Services to be Provided (App. G)**

Note: on App. G Detailed Technical and Functional Requirements Excel spreadsheet, a tab is labeled User Stories. No response is required for Tab 3; these were provided to bidders for clarity and understanding of the expected journey a Constituent will experience.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: PruTech
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes:P	**1. System security components System security must include the following security components:**
	1) Account Take Over Protections
	a) Account Sign-in Protections
	a) Account Sign-in Protections
	a) Adaptive AI Technology
	b) Bot Protection: identify visitor behavior through analysis of technical and behavioral data.
☒ P, Q, N or I Notes: P	**2. Identity Proofing must have the ability to provide levels of proofing which will be directly tied to the constituent's level of access.**
	1) Define various levels of id proofing
	2) Document Image Capture
	3) Close coupling with authentication
☒ P, Q, N or I Notes: P	**3. Multi-factor authentication The system must support multi-factor authentication to protect against user impersonation and credential theft.**
☒ P, Q, N or I Notes: P	**4. Risk-based factors The system must support risk-based factors and scores that are based on factors such as, but not limited to, device and location.**
☒ P, Q, N or I Notes: P	**5. Identity lifecycle management components The system must include the following identity lifecycle management components for risk-based critical applications not limited to end users but also for generic accounts and system/service accounts:**
P	1) Identity Creation
P	2) Identity provisioning
P	3) Attribute maps
P	4) Authentication (e.g., password policies and synchronization)

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: PruTech
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes:P	**6. Security event logging The system must log security information and events.**
	Security Information and Event Management (SIEM) – Splunk
	Cloud Services: Azure, AWS, Oracle, Google
☒ P, Q, N or I Notes:P	**7. Security Certifications The system must comply too or have the following security certifications:**
P	1) NIST 800-53
P	2) FedRamp
P	3) HIPAA
P	4) SOC 2 Type II
	Note:
	IRS require a 45-day letter approval for new cloud solutions.
☒ P, Q, N or I Notes:P	**8. SIEM (Splunk) integration The system must be able to integrate with the State of Maine Security Information and Event Monitoring (SIEM) Splunk for Security Operations Center operations.**
☒ P, Q, N or I Notes:P	**9. Core constituent data. The system must maintain a central repository of basic (core) constituent data, that can be used by any SoM application to reduce data redundancy and outdated or inaccurate information while maintaining confidentiality.**
☒ P, Q, N or I Notes:P	**11. Data Management. The system must apply the Data Management Rules to the constituent profile data as per the SoM Data Management Policies.**
☒ P, Q, N or I Notes:P	**12. SOM Employee. The system must support multiple identities for SOM employees that work with the portal in a support role.**
P	1) SOM Employee identity and credentials for supporting the application.

P	2) Constituent identity and credentials to use the state services offered through the portal.

☒ P, Q, N or I Notes:	**13. APIs. The system must be able to connect to at least one agency application.**
	Considerations:
	a) OpenID, OAuth, WS-Fed, SAML, LDAP, Active Directory, Application Programming Interfaces (APIs), Software Development
	b) Develop once and reuse often with other agencies would be ideal
☒ P, Q, N or I Notes:P	**14. User identification matching. The system must be able to match the identity of the portal user to the identity of the same user in the agency system.**
☒ P, Q, N or I Notes:P	**15. Single sign-on. The system must support single sign-on to the agency application.**
☒ P, Q, N or I Notes:P	**16. Import user profile data from agency systems. The system must be able to import user data from different SoM applications to ensure offboarding happens in a timely manner, so that government resources are protected from fraud. (example: death records)**
☒ P, Q, N or I Notes:P	**17. History logging.** 1) The system must log all actions taken by:
P	a) Constituents
P	b) MaineIT support
	Including but not limited to:
P	c) who made the change
P	d) when the change was made
P	e) what changed

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: PruTech
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes:Q doesn't say in portal visible.	**18. Reporting. The logging data (history) must be available for constituent and system dashboards and reporting in general.**
☒ P, Q, N or I Notes:P	**19. Security Controls. The system must comply to the following security controls:**
P	1) DDOS Protections[WN1] ,
P	2) OWASP Top 10
P	a) Cross Site Scripting,
P	b) SQL Injection,
P	3) Authentication bypass,
P	a) poorly authenticated APIs,
P	b) Role based access controls,
P	c) proper session control
P	4) Real-time visibility,
P	5) Anomalous behavior,
P	6) User sign with geo-location tracking,
P	Geo-blocking capabilities.
P	Security controls must include Web Application Firewall [WN1]
☒ P, Q, N or I Notes:P	**20. General System Requirements.** 1) Mobile Support with Native App; (iOS and Android)
P	2) System availability: 24/7 with 4x1-hour outages per year
P	3) Identity relationships must be tracked in the cloud infrastructure.
P	4) Support responsive web and web browsers.
P	a. Supports Windows, Chrome, and Macintosh operating systems
☒	**21. Training and Support.**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: PruTech
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

P, Q, N or I Notes:P	1) Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
P	2) MaineIT will require technical/administrator training. There will be initial training and on-going training as users are added.
P	3) Have a continuous process to ensure constituents that may have run into issues setting up accounts can have help 24/7.
☒ P, Q, N or I Notes:P	**22. Support Requirements** 1) The Bidder will provide support, and maintenance for the solution to begin immediately after receiving the State's official acceptance of the implemented solution.
P	2) Support and maintenance will be provided for the terms and duration specified in the contract.
P	3) The Bidder will address all questions and reported problems related to the technical and functional operation of the system.
P	4) The Bidder must provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours: 8:00 a.m. to 5:00 p.m. Eastern Standard Time.
P	5) As part of the maintenance agreement, the Bidder will make all product releases and upgrades available to the State at no additional charge.
P	6) All release and upgrades shall be implemented and tested by the Bidder, outside of the normal operating hours of the State government.
P	7) User testing shall occur during normal State business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State government.
☒ P, Q, N or I Notes:P	**23. Hosting** Solution can comply with MaineIT remote hosting policies. a) Remote Hosting Policy http://maine.gov/oit/policies/RemoteHostingPolicy.pdf b) Hosting Customization Policy http://maine.gov/oit/policies/HostingCustomizationPolicy.pdf
☒ P, Q, N or I	**24. Disaster Recovery** Proposed Solution can comply with MaineIT security requirements and remote hosting requirements, without requiring waivers, before contract finalization.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: PruTech
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

Notes:P	
P	1) Maintaining an availability metric of ninety-nine-point nine percent (99.9%) of uptime
P	2) Ensuring the capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six hours (i.e., maximum data loss cannot exceed six (6) hours);
P	3) Ensuring a recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours;
P	4) Ensuring the hosting environment provides adequate capacity to ensure that, under ethernet connectivity to the client device, data inquiry/lookup response is within three (3) seconds, and data modification response is within five (5) seconds;
P	5) Providing the Department at least thirty (30) calendar day advance written notice of any material change in network operations or architecture;
P	6) Ensuring any planned material change in network operations or architecture cannot be made without the prior written consent of the Department; and Outlining of all Service Level Agreements (SLAs) for technical support (the awarded Bidder shall be open to negotiation to ensure the SLAs meet the Department's needs

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

☒1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
P, N, Q, or I & Notes:

☒1b) Detailed description of the technologies, software and / or hardware for each of the components.
P, N, Q, or I & Notes:P

☒1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.

P, N, Q, or I & Notes:P

☒1d) Description of the overall platform and architecture of the proposed solution(s).
P, N, Q, or I & Notes:P

☒1e) Description of any third-party software or partnerships required for the proposed Solution(s).
P, N, Q, or I & Notes:P

☒2a) A detailed timeline and description of milestones, deliverables, tasks
P, N, Q, or I & Notes:P

☒2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period
P, N, Q, or I & Notes:P

☒2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
P, N, Q, or I & Notes:P

☒2d) Average time to market for each component.
P, N, Q, or I & Notes:Q don't see average time to market for each component

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. ☒Capture Constituent Identity and profile data.

P, N, Q, or I & Notes:P

b. ☒Provide identity provisioning and deprovisioning.
P, N, Q, or I & Notes:P

c. ☒Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
   i. Identity Creation
   ii. Identity provisioning
   iii. Attribute maps
   iv. Authentication (e.g., password policies and synchronization)
      P, N, Q, or I & Notes:P

d. ☒Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies. P
P, N, Q, or I & Notes:

e. ☒Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
P, N, Q, or I & Notes:P

f. ☒Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.
P, N, Q, or I & Notes:P

g. ☒Allow for multiple role selections for the following identities:
   i. Individual
   ii. Business Owner
   iii. Support multiple identities for State employees that work with the portal in a support role:
      (a) SOM Employee identity and credentials for supporting the application.
      (b) Constituent identity and credentials to use the state services offered through the portal.
   iv. Multi role individual (Individual and Business Owner)
      P, N, Q, or I & Notes:P

h. ☒Have the ability to provide levels of proofing which will be directly tied to the Constituent's level of consent given.
P, N, Q, or I & Notes:p

i. ☒Support multi-factor authentication to protect against user impersonation and credential theft.
P, N, Q, or I & Notes:P

B.2. ☒The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.
P, N, Q, or I & Notes:P

a. Disclosure and Consent Management

The desire of the State is to be as transparent as possible and respect the privacy of the individual interacting with the Constituents' Portal. Consent is a core tenant of maintaining the public trust in the Constituents' Portal and will be a foundational component of the architecture.

The Disclosure and Consent Management solution shall include:

i. ☒Granular consent management that encompasses the automated functions necessary to create, modify, revoke, and manage Constituent consents.
ii. ☒Allow users the ability to opt-in and opt-out of data sharing and services within the Constituents' portal.
iii. ☒Obtain user consent both in an interactive and set preference mode for a variety of transactions on the Portal.
iv. ☒Support administrative users' management of standard legal disclaimers and data classification for transactions.
v. ☒Highly configurable with version control and history tracking for consent language.
vi. ☒Ability for end user to access a retrievable log of granted consent and data usage on the portal derived from the consent.

P, N, Q, or I & Notes:P

b. Recommendation Technology

The State is seeking options which, while maintaining individual privacy, will collect and analyze data about user interactions, behavior, and preferences. The

expected outcome of this will be to provide insights and intelligence that help the State make informed decisions and improve Constituent experiences.

- i. ☒From the user perspective, the portal should be able to make real-time recommendations for related services.
- ii. ☒Data captured in this environment must be obfuscated, as to not allow any party to directly target or track the preferences of an individual or their usage of the portal.
- iii. ☒Solution providers should discuss in detail their use, storage, destruction of metadata, and tracking technologies with emphasis on how their offering provides analytical insights while protecting the individual user privacy.

P, N, Q, or I & Notes:P

c. Data Management

The State is seeking the ability for the portal's Constituent identity to be linked to records maintained by individual State agencies. The proposed solution will include:

- i. ☒Capabilities to streamline the sharing of data between State systems, including
  - i. The identity assurance level
  - ii. Agency to user notifications
  - iii. Verification of user consent
  - iv. Identity resolution
  - v. Data sharing between agencies.
- ii. ☒Maintain a central repository of basic (core) Constituent data, that can be used by any State application to reduce data redundancy, and outdated or inaccurate information while maintaining confidentiality.
- iii. ☒Ability to integrate with State applications using, OpenID, OAuth, Web Services Federation Protocol (WS-Fed), Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), Active Directory, Application Programming Interface (API) or equivalent protocols.
- iv. ☒Ability to match the identity of the portal user to the identity of the same user in the Agency system.
- v. ☒Log all actions taken by:
  - i. Constituents
  - ii. MaineIT Support, including:
    - (a) Who made the change
    - (b) When the change was made

(c) What changed to and from

vi. ☒Logging data must be available for system dashboards and reporting.

P, N, Q, or I & Notes:P

d. Customer Service

The State is seeking solution(s) to provide 24/7/365 customer service to Constituents regardless of their location or technical abilities.

  i. ☒Support Constituents with personalized and timely assistance.
  ii. ☒Provide the state options to support our Constituents across multiple channels including, but not limited to phone, email, chat, etc.

P, N, Q, or I & Notes: P

C.1. General System

  a. ☒Mobile support with native app (iOS and Android)
  b. ☒System availability: 24/7 with a maximum of four (4) 1-hour outages per year
  c. ☒Identity relationships must be tracked in the cloud infrastructure.
  d. ☒Support responsive web and web browsers.
    i. ☒Supports Windows, Chrome, and Macintosh operating systems.

P, N, Q, or I & Notes:Q doesn’t mention mobile compatibility with Dashboard.

C.2. ☒Compliance with MaineIT Policies & Standards

  a. Architecture Compliance Policy
  b. System and Services Acquisition Policy and Procedures (SA-1)
  c. Application Deployment Certification Policy
  d. Digital Accessibility Policy
  e. Remote Hosting Policy
  f. Data Exchange Policy
  g. Information Security Policy
  h. Access Control Policy (AC-1)
  i. Access Control Procedures for Users (AC-2)
  j. Risk Assessment Policy and Procedures (RA-1)
  k. Vulnerability Scanning Procedure (RA-5)
  l. Security Assessment and Authorization Policy and Procedures (CA-1)
  m. System and Information Integrity Policy and Procedures (SI-1)

n. Configuration Management Policy (CM-1)
o. Web Standards

P, N, Q, or I & Notes:P

C.3. Support and Maintenance

a. ☒Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State's official acceptance of the implemented solution.
P, N, Q, or I & Notes:P
b. ☒Terms and duration of the support and maintenance will be specified in the contract.
P, N, Q, or I & Notes:P

c. ☒All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
P, N, Q, or I & Notes:P
d. ☒Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
P, N, Q, or I & Notes:P
e. ☒All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
P, N, Q, or I & Notes:P
f. ☒All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
P, N, Q, or I & Notes:P
g. ☒User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
P, N, Q, or I & Notes:P

4. Security

The proposed solutions must provide a robust security system that aligns with the States Security Policies, standards, and Processes, Including:

Comply with or have the following security certifications:

i. ☒National Institute of Standards and Technology (NIST) 800-53
ii. ☒FedRamp
iii. ☒Health Insurance Portability and Accountability Act (HIPAA)
iv. ☒SOC 2 Type II
v. ☒Comply to the following security controls:
vi. ☒DDOS Protections [WN1]
vii. ☒Open Web Application Security Project (OWASP) Top 10
viii. ☒Cross Site Scripting
ix. ☒Structured Query Language (SQL) Injection
x. ☒Authentication bypass
xi. ☒Poorly authenticated APIs
xii. ☒Role based access controls
xiii. ☒Proper session control
xiv. ☒Real-time visibility
xv. ☒Anomalous behavior
xvi. ☒User sign with geo-location tracking
xvii. ☒Geo-blocking capabilities.
xviii. ☒Web Application Firewall [WN1]
xix. ☒System security must include the following security components:
xx. ☒Account take over protections
xxi. ☒Account sign-in Protections
xxii. ☒Behavior detection and evaluation
xxiii. ☒Adaptive AI Technology
xxiv. ☒Bot Protection; identity visitor behavior through analysis, technical and behavioral data.
xxv. ☒The proposed solution must be able to integrate with the State Security Information and Event Monitoring (SIEM) Splunk. Ability to log security information and events.

P, N, Q, or I & Notes:P

5. Licensing

☒The State is aware that multiple licensing options are available and will be required to support the proposed solution in its entirety. The State seeks bids which will provide the most cost-effective licensing approach. Bidders are required to provide a detail breakdown for the proposed licensing.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: PruTech
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

P, N, Q, or I & Notes:P

1. Training and OCM (Organizational Change Management)

a. ☒Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
b. ☒Training must include technical and administrator training, initial and ongoing as users are added.
c. ☒Continuous process to ensure Constituents that may have run into issues setting up accounts have help 24/7.
d. ☒Bidders shall guide the State in OCM engagement for the duration of project planning, transition, and final implementation phase including:
    i. Designing and managing team structures with roles and responsibilities to facilitate automated program delivery, while noting any risks anticipated from the lack of readiness in the organization and staffing.
    ii. Ensure a successful transition for the integration of new processes and technology with stakeholders.
    iii. Organizational readiness assessment

P, N, Q, or I & Notes:P

3. Disaster Recovery

a. ☒Availability of ninety-nine-point nine percent (99.9%) of uptime
b. ☒Capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six (6) hours (i.e., maximum data loss cannot exceed six (6) hours)
c. ☒Recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours.

P, N, Q, or I & Notes:P

4. Feature Enhancements

a. ☒The State is seeking two hundred and fifty (250) hours of time and material for each proposed technology (CIAM), Personalized Dashboard, Disclosure and Consent Management, Data Management, and Recommendation Technology) to allow for specifications and enhancements during the contract period.

P, N, Q, or I & Notes:P

5. Project Management

a. ☒The State plans to have its own project manager however, the awarded Bidder must have a project manager that has the primary responsibility for executing the project management tasks associated with the project. The awarded Bidder will:
   i. Work in collaboration with the State's Project Manager
   ii. Align with State Project Management processes and practices.

b. ☒Manage the implementation, executing all activities, tasks, deliverables and resource needs, both state and awarded Bidder.

c. ☒Track project status including managing and tracking all project risks, issues and decisions.

d. ☒Track and report status of deliverables and project status

e. ☒The awarded Bidder will provide their approach for project management and administration services including:
   i. Project Management Methodology
   ii. Project Governance
   iii. Resource Allocation and Schedule Management approach
   iv. Communication Management Approach including status reporting and document repository management.
   v. Risk and Issue Management Methodology
   vi. Change Management Methodology
   vii. Quality Management Methodology

P, N, Q, or I & Notes:P

D. Value Added Options (Other)

☒Bidders shall provide value added optional services to address relevant matters that have not been anticipated in this RFP but contribute to successful implementation of the proposed solutions, as well as any technology or services that will reduce risk to the project's quality and continuity. The value-added technology and services will not be included in the evaluation process but may be added during the contract negotiations.

P, N, Q, or I & Notes:P

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: PruTech
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: PruTech
DATE: 05 June 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: MaineIT

Section I – Preliminary Information (No points – Eligibility Requirements)

(File #1 App. A, B, C)
☒Done – Pass/Fail by Procurement & RFP Coordinator

Section II Organization Qualifications and Experience

(File #2 – App. D, E + other areas that have no Appendix number but are part of File #2)

1. **Overview of the Organization (App. D)**
   ☒Bidders must include three examples of projects which demonstrate their experience and expertise in performing these services as well as highlighting the Bidder's stated qualifications and skills.
   P: Strong response
   Q: Six examples, instead of three

   Statement of qualifications
   ☒Client name, contact person, Ph#, email.
   Contract history with the state may be considered in rating proposals even if not provided by the bidder.
   P: Strong response

2. **Subcontractors (App. E)**
   ☒If subcontractors are to be used, Bidders must provide the name, address, phone number, contact person, and a brief description of the subcontractors' organizational capacity and qualifications.
   Business name, contact person, address, ph#, email.
   P: Two subcontractors (PontisResearch & Cybolt)). All details provided.

3. **Organizational Chart (No Appendix)**
   ☒Bidders must provide an organizational chart. The organizational chart must include the project being proposed. Each position must be identified by position title and corresponding to the personnel job descriptions.
   P: Strong response

4. **Litigation (No App.)**
   ☒Bidders must attach a list of all current litigation in which the Bidder is named and a list of all closed cases that have closed within the past five (5) years in which the

Bidder paid the claimant either as part of a settlement or by decree. For each, list the entity bringing suit, the complaint, the accusation, amount, and outcome.
P: No Litigation
P: Strong response

5. **Financial Viability (No App.)**
☒Bidders must provide a current copy of their Dun & Bradstreet Business Information Report Snapshot.
P: Strong response

6. **Licensure/Certification (No App.)**
☒Bidders *may* provide documentation of any applicable licensure/certification or specific credentials that are related to providing the proposed services of the RFP.
P: Strong response (CMMI Lev 3, ISO 9001:2015, SOC 2 Type 2)

7. **Certificate of Insurance (No App.)**
☒Bidders must provide a certificate of insurance on a standard ACORD form (or the equivalent) evidencing the Bidder's general liability, professional liability and any other relevant liability insurance policies that might be associated with the proposed services.
P: $10 M Cyber Liability

Section III - Proposed Services

(File #3 – App. F, G, H)

1. **Technical Assessment (App. F)**
☒Done

2. **Services to be Provided (App. G)**

Note: on App. G Detailed Technical and Functional Requirements Excel spreadsheet, a tab is labeled User Stories. No response is required for Tab 3; these were provided to bidders for clarity and understanding of the expected journey a Constituent will experience.

☒ *P: Strong response*	**1. System security components System security must include the following security components:**	
	1)	Account Take Over Protections
	a)	Account Sign-in Protections

	a) Account Sign-in Protections
	a) Adaptive AI Technology
	b) Bot Protection: identify visitor behavior through analysis of technical and behavioral data.
☒ *P: Strong response*	**2. Identity Proofing must have the ability to provide levels of proofing which will be directly tied to the constituent's level of access.**
	1) Define various levels of id proofing
	2) Document Image Capture
	3) Close coupling with authentication
☒ *P: Strong response*	**3. Multi-factor authentication The system must support multi-factor authentication to protect against user impersonation and credential theft.**
☒ *P: Strong response*	**4. Risk-based factors The system must support risk-based factors and scores that are based on factors such as, but not limited to, device and location.**
☒ *P: Strong response*	**5. Identity lifecycle management components The system must include the following identity lifecycle management components for risk-based critical applications not limited to end users but also for generic accounts and system/service accounts:**
	1) Identity Creation
	2) Identity provisioning
	3) Attribute maps
	4) Authentication (e.g., password policies and synchronization)
☒ *N: Weak response. No mention of the actual products.*	**6. Security event logging The system must log security information and events.**
	Security Information and Event Management (SIEM) – Splunk

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: PruTech
DATE: 05 June 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: MaineIT

	Cloud Services: Azure, AWS, Oracle, Google
☒ *P: Adequate response* *N: Did NOT ack the IRS 45-day notice*	**7. Security Certifications The system must comply too or have the following security certifications:**
	1) NIST 800-53
	2) FedRamp
	3) HIPAA
	4) SOC 2 Type II
	Note:
	IRS require a 45-day letter approval for new cloud solutions.
☒ *P: Adequate response*	**8. SIEM (Splunk) integration The system must be able to integrate with the State of Maine Security Information and Event Monitoring (SIEM) Splunk for Security Operations Center operations.**
☒ *N: Weak response (Covers Okta, but NOT Thales)*	**9. Core constituent data. The system must maintain a central repository of basic (core) constituent data, that can be used by any SoM application to reduce data redundancy and outdated or inaccurate information while maintaining confidentiality.**
☒ *P: Even though marked Partial, Adequate response*	**11. Data Management. The system must apply the Data Management Rules to the constituent profile data as per the SoM Data Management Policies.**
☒ *P: Adequate response*	**12. SOM Employee. The system must support multiple identities for SOM employees that work with the portal in a support role.**
	1) SOM Employee identity and credentials for supporting the application.
	2) Constituent identity and credentials to use the state services offered through the portal.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: PruTech
DATE: 05 June 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: MaineIT

☒ *P: Strong response*	**13. APIs. The system must be able to connect to at least one agency application.**
	Considerations:
	a) OpenID, OAuth, WS-Fed, SAML, LDAP, Active Directory, Application Programming Interfaces (APIs), Software Development
	b) Develop once and reuse often with other agencies would be ideal
☒ *P: Strong response*	**14. User identification matching. The system must be able to match the identity of the portal user to the identity of the same user in the agency system.**
☒ *P: Strong response*	**15. Single sign-on. The system must support single sign-on to the agency application.**
☒ *P: Adequate response*	**16. Import user profile data from agency systems. The system must be able to import user data from different SoM applications to ensure offboarding happens in a timely manner, so that government resources are protected from fraud. (example: death records)**
☒ *N: Weak response (No mention of actual products)*	**17. History logging.** 1) The system must log all actions taken by:
	a) Constituents
	b) MaineIT support
	Including but not limited to:
	c) who made the change
	d) when the change was made
	e) what changed
☒ *N: Weak response*	**18. Reporting. The logging data (history) must be available for constituent and system dashboards and reporting in general.**

(Covers Okta, but NOT Thales)	
☒ *N: Weak response (Covers Okta, but NOT Thales)*	**19. Security Controls. The system must comply to the following security controls:**
	1) DDOS Protections[WN1] ,
	2) OWASP Top 10
	a) Cross Site Scripting,
	b) SQL Injection,
	3) Authentication bypass,
	a) poorly authenticated APIs,
	b) Role based access controls,
	c) proper session control
	4) Real-time visibility,
	5) Anomalous behavior,
	6) User sign with geo-location tracking,
	Geo-blocking capabilities.
	Security controls must include Web Application Firewall [WN1]
☒ *P: Adequate response*	**20. General System Requirements.** 1) Mobile Support with Native App; (iOS and Android)
	2) System availability: 24/7 with 4x1-hour outages per year
	3) Identity relationships must be tracked in the cloud infrastructure.
	4) Support responsive web and web browsers.
	a. Supports Windows, Chrome, and Macintosh operating systems
☒	**21. Training and Support.**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: PruTech
DATE: 05 June 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: MaineIT

P: Adequate response (Details at discovery)	1) Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
	2) MaineIT will require technical/administrator training. There will be initial training and on-going training as users are added.
	3) Have a continuous process to ensure constituents that may have run into issues setting up accounts can have help 24/7.
☒ *P: Adequate response (Details at discovery)*	**22. Support Requirements** 1) The Bidder will provide support, and maintenance for the solution to begin immediately after receiving the State's official acceptance of the implemented solution.
	2) Support and maintenance will be provided for the terms and duration specified in the contract.
	3) The Bidder will address all questions and reported problems related to the technical and functional operation of the system.
	4) The Bidder must provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours: 8:00 a.m. to 5:00 p.m. Eastern Standard Time.
	5) As part of the maintenance agreement, the Bidder will make all product releases and upgrades available to the State at no additional charge.
	6) All release and upgrades shall be implemented and tested by the Bidder, outside of the normal operating hours of the State government.
	7) User testing shall occur during normal State business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State government.
☒ *N: Adequate response*	**23. Hosting** Solution can comply with MaineIT remote hosting policies. a) Remote Hosting Policy http://maine.gov/oit/policies/RemoteHostingPolicy.pdf b) Hosting Customization Policy http://maine.gov/oit/policies/HostingCustomizationPolicy.pdf

☒ *P: Weak response (Only covers Okta, NOT Thales)*	**24. Disaster Recovery** Proposed Solution can comply with MaineIT security requirements and remote hosting requirements, without requiring waivers, before contract finalization.
	1) Maintaining an availability metric of ninety-nine-point nine percent (99.9%) of uptime
	2) Ensuring the capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six hours (i.e., maximum data loss cannot exceed six (6) hours);
	3) Ensuring a recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours;
	4) Ensuring the hosting environment provides adequate capacity to ensure that, under ethernet connectivity to the client device, data inquiry/lookup response is within three (3) seconds, and data modification response is within five (5) seconds;
	5) Providing the Department at least thirty (30) calendar day advance written notice of any material change in network operations or architecture;
	6) Ensuring any planned material change in network operations or architecture cannot be made without the prior written consent of the Department; and Outlining of all Service Level Agreements (SLAs) for technical support (the awarded Bidder shall be open to negotiation to ensure the SLAs meet the Department's needs

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

☒1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
P: Strong response

☒1b) Detailed description of the technologies, software and / or hardware for each of the components.
P: Strong response

☒1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.
P: Strong response

☒1d) Description of the overall platform and architecture of the proposed solution(s).
P: Strong response

☒1e) Description of any third-party software or partnerships required for the proposed Solution(s).
P: Strong response

☒2a) A detailed timeline and description of milestones, deliverables, tasks
P: Strong response

☒2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period
P: Strong response

☐2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
P: NO response

☐2d) Average time to market for each component.
P: NO response

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. ☒Capture Constituent Identity and profile data.
   P: Strong response

b. ☒Provide identity provisioning and deprovisioning.
   P: Strong response

c. ☒Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
   i. Identity Creation
   ii. Identity provisioning
   iii. Attribute maps
   iv. Authentication (e.g., password policies and synchronization)
      P: Strong response

d. ☒Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies.
   P: Strong response

e. ☒Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
   P: Strong response

f. ☒Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.
   N: Strong response

g. ☒Allow for multiple role selections for the following identities:
   i. Individual
   ii. Business Owner
   iii. Support multiple identities for State employees that work with the portal in a support role:
      (a) SOM Employee identity and credentials for supporting the application.
      (b) Constituent identity and credentials to use the state services offered through the portal.
   iv. Multi role individual (Individual and Business Owner)
   N: Strong response

h. ☒Have the ability to provide levels of proofing which will be directly tied to the Constituent's level of consent given.
   N: Weak response. Did NOT mention Thales.

i. ☒Support multi-factor authentication to protect against user impersonation and credential theft.
P: Strong response

B.2. ☒The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.
P: Strong response

a. Disclosure and Consent Management
The desire of the State is to be as transparent as possible and respect the privacy of the individual interacting with the Constituents' Portal. Consent is a core tenant of maintaining the public trust in the Constituents' Portal and will be a foundational component of the architecture.
The Disclosure and Consent Management solution shall include:

i. ☒Granular consent management that encompasses the automated functions necessary to create, modify, revoke, and manage Constituent consents.
P: Adequate response

ii. ☒Allow users the ability to opt-in and opt-out of data sharing and services within the Constituents' portal.
P: Adequate response

iii. ☒Obtain user consent both in an interactive and set preference mode for a variety of transactions on the Portal.
P: Adequate response

iv. ☒Support administrative users' management of standard legal disclaimers and data classification for transactions.
P: Adequate response

v. ☒Highly configurable with version control and history tracking for consent

language.
P: Adequate response

vi. ☒Ability for end user to access a retrievable log of granted consent and data usage on the portal derived from the consent.
P: Adequate response

b. Recommendation Technology

The State is seeking options which, while maintaining individual privacy, will collect and analyze data about user interactions, behavior, and preferences. The expected outcome of this will be to provide insights and intelligence that help the State make informed decisions and improve Constituent experiences.

i. ☒From the user perspective, the portal should be able to make real-time recommendations for related services.
P: Strong response

ii. ☒Data captured in this environment must be obfuscated, as to not allow any party to directly target or track the preferences of an individual or their usage of the portal.
P: Strong response

iii. ☒Solution providers should discuss in detail their use, storage, destruction of metadata, and tracking technologies with emphasis on how their offering provides analytical insights while protecting the individual user privacy.
P: Strong response

c. Data Management

The State is seeking the ability for the portal's Constituent identity to be linked to records maintained by individual State agencies. The proposed solution will include:

i. ☒Capabilities to streamline the sharing of data between State systems, including
    i. The identity assurance level
    ii. Agency to user notifications
    iii. Verification of user consent
    iv. Identity resolution
    v. Data sharing between agencies.
P: Strong response

ii. ☒Maintain a central repository of basic (core) Constituent data, that can be used by any State application to reduce data redundancy, and outdated or inaccurate information while maintaining confidentiality.
P: Strong response

iii. ☒Ability to integrate with State applications using, OpenID, OAuth, Web Services Federation Protocol (WS-Fed), Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), Active Directory, Application Programming Interface (API) or equivalent protocols.
P: Strong response

iv. ☒Ability to match the identity of the portal user to the identity of the same user in the Agency system.
P: Strong response

v. ☒Log all actions taken by:
   i. Constituents
   ii. MaineIT Support, including:
      (a) Who made the change
      (b) When the change was made
      (c) What changed to and from
N: Weak response (Covers Okta, but NOT Thales)

vi. ☒Logging data must be available for system dashboards and reporting.
N: Weak response (Covers Okta, but NOT Thales)

d. Customer Service
The State is seeking solution(s) to provide 24/7/365 customer service to Constituents regardless of their location or technical abilities.
   i. ☒Support Constituents with personalized and timely assistance.
   ii. ☒Provide the state options to support our Constituents across multiple channels including, but not limited to phone, email, chat, etc.
P: Strong response
Q: Was it included in the Cost Proposal?

C.1. General System
   a. ☒Mobile support with native app (iOS and Android)
   b. ☒System availability: 24/7 with a maximum of four (4) 1-hour outages per

year

c. ☒Identity relationships must be tracked in the cloud infrastructure.

d. ☒Support responsive web and web browsers.
   i. ☒Supports Windows, Chrome, and Macintosh operating systems.

N: Weak response (Covers Okta, but NOT Thales)

C.2. ☒Compliance with MaineIT Policies & Standards

a. Architecture Compliance Policy
b. System and Services Acquisition Policy and Procedures (SA-1)
c. Application Deployment Certification Policy
d. Digital Accessibility Policy
e. Remote Hosting Policy
f. Data Exchange Policy
g. Information Security Policy
h. Access Control Policy (AC-1)
i. Access Control Procedures for Users (AC-2)
j. Risk Assessment Policy and Procedures (RA-1)
k. Vulnerability Scanning Procedure (RA-5)
l. Security Assessment and Authorization Policy and Procedures (CA-1)
m. System and Information Integrity Policy and Procedures (SI-1)
n. Configuration Management Policy (CM-1)
o. Web Standards

N: Weak response (Covers Okta, but NOT Thales)

C.3. Support and Maintenance

a. ☒Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State’s official acceptance of the implemented solution.
P: Adequate response

b. ☒Terms and duration of the support and maintenance will be specified in the contract.
P: Adequate response

c. ☒All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
P: Adequate response

d. ☒Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
P: Adequate response

e. ☒All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
P: Adequate response

f. ☒All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
P: Adequate response

g. ☒User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
P: Adequate response

4. Security

The proposed solutions must provide a robust security system that aligns with the States Security Policies, standards, and Processes, Including:

Comply with or have the following security certifications:

i. ☒National Institute of Standards and Technology (NIST) 800-53
ii. ☒FedRamp
iii. ☒Health Insurance Portability and Accountability Act (HIPAA)
iv. ☒SOC 2 Type II
v. ☒Comply to the following security controls:
vi. ☒DDOS Protections [WN1]
vii. ☒Open Web Application Security Project (OWASP) Top 10
viii. ☒Cross Site Scripting
ix. ☒Structured Query Language (SQL) Injection
x. ☒Authentication bypass
xi. ☒Poorly authenticated APIs
xii. ☒Role based access controls
xiii. ☒Proper session control
xiv. ☒Real-time visibility

xv. ☒Anomalous behavior
xvi. ☒User sign with geo-location tracking
xvii. ☒Geo-blocking capabilities.
xviii. ☒Web Application Firewall [WN1]
xix. ☒System security must include the following security components:
xx. ☒Account take over protections
xxi. ☒Account sign-in Protections
xxii. ☒Behavior detection and evaluation
xxiii. ☒Adaptive AI Technology
xxiv. ☒Bot Protection; identity visitor behavior through analysis, technical and behavioral data.
xxv. ☒The proposed solution must be able to integrate with the State Security Information and Event Monitoring (SIEM) Splunk. Ability to log security information and events.

N: Weak response (Covers Okta, but NOT Thales)

5. Licensing

☒The State is aware that multiple licensing options are available and will be required to support the proposed solution in its entirety. The State seeks bids which will provide the most cost-effective licensing approach. Bidders are required to provide a detail breakdown for the proposed licensing.

P: Adequate response

1. Training and OCM (Organizational Change Management)

a. ☒Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
b. ☒Training must include technical and administrator training, initial and ongoing as users are added.
c. ☐Continuous process to ensure Constituents that may have run into issues setting up accounts have help 24/7.
d. ☒Bidders shall guide the State in OCM engagement for the duration of project planning, transition, and final implementation phase including:
   i. Designing and managing team structures with roles and responsibilities to facilitate automated program delivery, while noting any risks anticipated from the lack of readiness in the organization and staffing.
   ii. Ensure a successful transition for the integration of new processes and technology with stakeholders.

        iii. Organizational readiness assessment

N: NO response to c
P: Otherwise, Adequate response

3. **Disaster Recovery**
    a. ☒Availability of ninety-nine-point nine percent (99.9%) of uptime
    b. ☒Capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six (6) hours (i.e., maximum data loss cannot exceed six (6) hours)
    c. ☒Recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours.

    N: Weak response (Covers Okta, but NOT Thales)

4. **Feature Enhancements**

a. ☒The State is seeking two hundred and fifty (250) hours of time and material for each proposed technology (CIAM), Personalized Dashboard, Disclosure and Consent Management, Data Management, and Recommendation Technology) to allow for specifications and enhancements during the contract period.
P: Adequate response

5. **Project Management**
    a. ☐The State plans to have its own project manager however, the awarded Bidder must have a project manager that has the primary responsibility for executing the project management tasks associated with the project. The awarded Bidder will:
        i. Work in collaboration with the State’s Project Manager
        ii. Align with State Project Management processes and practices.
    b. ☐Manage the implementation, executing all activities, tasks, deliverables and resource needs, both state and awarded Bidder.
    c. ☐Track project status including managing and tracking all project risks, issues and decisions.
    d. ☐Track and report status of deliverables and project status
    e. ☒The awarded Bidder will provide their approach for project management and administration services including:
        i. Project Management Methodology
        ii. Project Governance
        iii. Resource Allocation and Schedule Management approach

iv. Communication Management Approach including status reporting and document repository management.
v. Risk and Issue Management Methodology
vi. Change Management Methodology
vii. Quality Management Methodology

N: NO response to a, b, c, d
P: Adequate response to e
N: Weak response overall

D. Value Added Options (Other)

☒Bidders shall provide value added optional services to address relevant matters that have not been anticipated in this RFP but contribute to successful implementation of the proposed solutions, as well as any technology or services that will reduce risk to the project's quality and continuity. The value-added technology and services will not be included in the evaluation process but may be added during the contract negotiations.

N: Irrelevant response

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: PruTech
DATE: 6/3/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

Section I – Preliminary Information (No points – Eligibility Requirements)

(File #1 App. A, B, C)

☒Done – Pass/Fail by Procurement & RFP Coordinator

Section II Organization Qualifications and Experience

(File #2 – App. D, E + other areas that have no Appendix number but are part of File #2)

1. Overview of the Organization (App. D)

☒Bidders must include three examples of projects which demonstrate their experience and expertise in performing these services as well as highlighting the Bidder's stated qualifications and skills.

Statement of qualifications

☒Client name, contact person, Ph#, email.

Contract history with the state may be considered in rating proposals even if not provided by the bidder.

P, N, Q, or I & Notes: P

2. Subcontractors (App. E)

☒If subcontractors are to be used, Bidders must provide the name, address, phone number, contact person, and a brief description of the subcontractors' organizational capacity and qualifications.

Business name, contact person, address, ph#, email.

P, N, Q, or I & Notes: P

3. Organizational Chart (No Appendix)

☒Bidders must provide an organizational chart. The organizational chart must include the project being proposed. Each position must be identified by position title and corresponding to the personnel job descriptions.

P, N, Q, or I & Notes - P

4. Litigation (No App.)

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: PruTech
DATE: 6/3/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

☒Bidders must attach a list of all current litigation in which the Bidder is named and a list of all closed cases that have closed within the past five (5) years in which the Bidder paid the claimant either as part of a settlement or by decree. For each, list the entity bringing suit, the complaint, the accusation, amount, and outcome.
P, N, Q, or I & Notes: P

5. **Financial Viability (No App.)**
☒Bidders must provide a current copy of their Dun & Bradstreet Business Information Report Snapshot.
P, N, Q, or I - Notes: P

6. **Licensure/Certification (No App.)**
☒Bidders *may* provide documentation of any applicable licensure/certification or specific credentials that are related to providing the proposed services of the RFP.
P, N, Q, or I & Notes: N -= Cost 2 Type 2 audit is out of date, it was through 8/23. ISO up to date. CMMI up to date.

7. **Certificate of Insurance (No App.)**
☒Bidders must provide a certificate of insurance on a standard ACORD form (or the equivalent) evidencing the Bidder's general liability, professional liability and any other relevant liability insurance policies that might be associated with the proposed services.
P, N, Q, or I & Notes: P

Section III - Proposed Services

(File #3 – App. F, G, H)

1. **Technical Assessment (App. F)**
☒Done

2. **Services to be Provided (App. G)**

Note: on App. G Detailed Technical and Functional Requirements Excel spreadsheet, a tab is labeled User Stories. No response is required for Tab 3; these were provided to bidders for clarity and understanding of the expected journey a Constituent will experience.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: PruTech
DATE: 6/3/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes: P	**1. System security components System security must include the following security components:**
	1) Account Take Over Protections
	a) Account Sign-in Protections
	a) Account Sign-in Protections
	a) Adaptive AI Technology
	b) Bot Protection: identify visitor behavior through analysis of technical and behavioral data.
☒ P, Q, N or I Notes: P	**2. Identity Proofing must have the ability to provide levels of proofing which will be directly tied to the constituent's level of access.**
	1) Define various levels of id proofing
	2) Document Image Capture
	3) Close coupling with authentication
☒ P, Q, N or I Notes: P	**3. Multi-factor authentication The system must support multi-factor authentication to protect against user impersonation and credential theft.**
☒ P, Q, N or I Notes: P	**4. Risk-based factors The system must support risk-based factors and scores that are based on factors such as, but not limited to, device and location.**
☒ P, Q, N or I Notes: P	**5. Identity lifecycle management components The system must include the following identity lifecycle management components for risk-based critical applications not limited to end users but also for generic accounts and system/service accounts:**
	1) Identity Creation
	2) Identity provisioning
	3) Attribute maps
	4) Authentication (e.g., password policies and synchronization)

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: PruTech
DATE: 6/3/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes: Q – if bidder indicates any cloud service choice of score, does that include the whole list being covered?	**6. Security event logging The system must log security information and events.**
	Security Information and Event Management (SIEM) – Splunk
	Cloud Services: Azure, AWS, Oracle, Google
☒ P, Q, N or I Notes: P	**7. Security Certifications The system must comply too or have the following security certifications:**
	1) NIST 800-53
	2) FedRamp
	3) HIPAA
	4) SOC 2 Type II
	Note:
	IRS require a 45-day letter approval for new cloud solutions.
☒ P, Q, N or I Notes: P	**8. SIEM (Splunk) integration The system must be able to integrate with the State of Maine Security Information and Event Monitoring (SIEM) Splunk for Security Operations Center operations.**
☒ P, Q, N or I Notes: P	**9. Core constituent data. The system must maintain a central repository of basic (core) constituent data, that can be used by any SoM application to reduce data redundancy and outdated or inaccurate information while maintaining confidentiality.**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: PruTech
DATE: 6/3/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes: P	**11. Data Management. The system must apply the Data Management Rules to the constituent profile data as per the SoM Data Management Policies.**
☒ P, Q, N or I Notes:	**12. SOM Employee. The system must support multiple identities for SOM employees that work with the portal in a support role.**
	1) SOM Employee identity and credentials for supporting the application.
	2) Constituent identity and credentials to use the state services offered through the portal.

☒ P, Q, N or I Notes: Q – bidder does not state that the system will connect to at least one	**13. APIs. The system must be able to connect to at least one agency application.**
	Considerations:
	a) OpenID, OAuth, WS-Fed, SAML, LDAP, Active Directory, Application Programming Interfaces (APIs), Software Development
	b) Develop once and reuse often with other agencies would be ideal
☒ P, Q, N or I Notes: P	**14. User identification matching. The system must be able to match the identity of the portal user to the identity of the same user in the agency system.**
☒ P, Q, N or I Notes: P	**15. Single sign-on. The system must support single sign-on to the agency application.**
☒ P, Q, N or I	**16. Import user profile data from agency systems. The system must be able to import user data from different SoM applications to ensure offboarding happens in a timely**

Notes: N – did not address protection from fraud, but did put a Y in the box	**manner, so that government resources are protected from fraud. (example: death records)**
☒ P, Q, N or I Notes: I - same answer for each area	**17. History logging.** 1) The system must log all actions taken by:
	a) Constituents
	b) MaineIT support
	Including but not limited to:
	c) who made the change
	d) when the change was made
	e) what changed
☒ P, Q, N or I Notes: N – did not address constituent dashboard	**18. Reporting. The logging data (history) must be available for constituent and system dashboards and reporting in general.**
☒ P, Q, N or I Notes: P	**19. Security Controls. The system must comply to the following security controls:**
	1) DDOS Protections[WN1] ,
	2) OWASP Top 10
	a) Cross Site Scripting,
	b) SQL Injection,
	3) Authentication bypass,
	a) poorly authenticated APIs,
	b) Role based access controls,

	c) proper session control
	4) Real-time visibility,
	5) Anomalous behavior,
	6) User sign with geo-location tracking,
	Geo-blocking capabilities.
	Security controls must include Web Application Firewall [WN1]
☒ P, Q, N or I Notes: N – did not address the 24/7, 4x1. Did not speak to identity relationships tracked in the cloud.	**20. General System Requirements.** 1) Mobile Support with Native App; (iOS and Android)
	2) System availability: 24/7 with 4x1-hour outages per year
	3) Identity relationships must be tracked in the cloud infrastructure.
	4) Support responsive web and web browsers.
	a. Supports Windows, Chrome, and Macintosh operating systems
☒ P, Q, N or I Notes: P	**21. Training and Support.** 1) Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
	2) MaineIT will require technical/administrator training. There will be initial training and on-going training as users are added.
	3) Have a continuous process to ensure constituents that may have run into issues setting up accounts can have help 24/7.
☒ P, Q, N or I P Notes:	**22. Support Requirements** 1) The Bidder will provide support, and maintenance for the solution to begin immediately after receiving the State's official acceptance of the implemented solution.

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: PruTech
DATE: 6/3/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

	2) Support and maintenance will be provided for the terms and duration specified in the contract.
	3) The Bidder will address all questions and reported problems related to the technical and functional operation of the system.
	4) The Bidder must provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours: 8:00 a.m. to 5:00 p.m. Eastern Standard Time.
	5) As part of the maintenance agreement, the Bidder will make all product releases and upgrades available to the State at no additional charge.
	6) All release and upgrades shall be implemented and tested by the Bidder, outside of the normal operating hours of the State government.
	7) User testing shall occur during normal State business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State government.
☒ P, Q, N or I Notes: P	**23. Hosting** Solution can comply with MaineIT remote hosting policies. a) Remote Hosting Policy http://maine.gov/oit/policies/RemoteHostingPolicy.pdf b) Hosting Customization Policy http://maine.gov/oit/policies/HostingCustomizationPolicy.pdf
☒ P, Q, N or I Notes: P	**24. Disaster Recovery** Proposed Solution can comply with MaineIT security requirements and remote hosting requirements, without requiring waivers, before contract finalization.
	1) Maintaining an availability metric of ninety-nine-point nine percent (99.9%) of uptime
	2) Ensuring the capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six hours (i.e., maximum data loss cannot exceed six (6) hours);
	3) Ensuring a recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours;
	4) Ensuring the hosting environment provides adequate capacity to ensure that, under ethernet connectivity to the client device,

	data inquiry/lookup response is within three (3) seconds, and data modification response is within five (5) seconds;
	5) Providing the Department at least thirty (30) calendar day advance written notice of any material change in network operations or architecture;
	6) Ensuring any planned material change in network operations or architecture cannot be made without the prior written consent of the Department; and Outlining of all Service Level Agreements (SLAs) for technical support (the awarded Bidder shall be open to negotiation to ensure the SLAs meet the Department's needs

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

☒1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
P, N, Q, or I & Notes: P

☒1b) Detailed description of the technologies, software and / or hardware for each of the components.
P, N, Q, or I & Notes: P

☒1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.
P, N, Q, or I & Notes: P

☒1d) Description of the overall platform and architecture of the proposed solution(s).
P, N, Q, or I & Notes: P

☒1e) Description of any third-party software or partnerships required for the proposed Solution(s).
P, N, Q, or I & Notes: P

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: PruTech
DATE: 6/3/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

☒2a) A detailed timeline and description of milestones, deliverables, tasks
P, N, Q, or I & Notes: P

☒2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period
P, N, Q, or I & Notes: P

☒2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
P, N, Q, or I & Notes: P

☒2d) Average time to market for each component.
P, N, Q, or I & Notes: P

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. ☒Capture Constituent Identity and profile data.
   P, N, Q, or I & Notes: P
b. ☒Provide identity provisioning and deprovisioning.
   P, N, Q, or I & Notes: P
c. ☒Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
   i. Identity Creation
   ii. Identity provisioning
   iii. Attribute maps
   iv. Authentication (e.g., password policies and synchronization)
      P, N, Q, or I & Notes: P

d. ☒Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies.
P, N, Q, or I & Notes: P

e. ☒Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
P, N, Q, or I & Notes: P

f. ☒Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.
P, N, Q, or I & Notes: P

g. ☒Allow for multiple role selections for the following identities:
  i. Individual
  ii. Business Owner
  iii. Support multiple identities for State employees that work with the portal in a support role:
    (a) SOM Employee identity and credentials for supporting the application.
    (b) Constituent identity and credentials to use the state services offered through the portal.
  iv. Multi role individual (Individual and Business Owner)
  P, N, Q, or I & Notes: P

h. ☒Have the ability to provide levels of proofing which will be directly tied to the Constituent's level of consent given.
P, N, Q, or I & Notes: P

i. ☒Support multi-factor authentication to protect against user impersonation and credential theft.
P, N, Q, or I & Notes: P

B.2. ☒The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.
P, N, Q, or I & Notes: P

a. Disclosure and Consent Management

The desire of the State is to be as transparent as possible and respect the privacy of the individual interacting with the Constituents' Portal. Consent is a core tenant of maintaining the public trust in the Constituents' Portal and will be a foundational component of the architecture.

The Disclosure and Consent Management solution shall include:

i. ☒Granular consent management that encompasses the automated functions necessary to create, modify, revoke, and manage Constituent consents.
ii. ☒Allow users the ability to opt-in and opt-out of data sharing and services within the Constituents' portal.
iii. ☒Obtain user consent both in an interactive and set preference mode for a variety of transactions on the Portal.
iv. ☒Support administrative users' management of standard legal disclaimers and data classification for transactions.
v. ☒Highly configurable with version control and history tracking for consent language.
vi. ☒Ability for end user to access a retrievable log of granted consent and data usage on the portal derived from the consent.

P, N, Q, or I & Notes: N – the only statement was that it is offered by their proposed solution without any detail.

b. Recommendation Technology

The State is seeking options which, while maintaining individual privacy, will collect and analyze data about user interactions, behavior, and preferences. The expected outcome of this will be to provide insights and intelligence that help the State make informed decisions and improve Constituent experiences.

i. ☒From the user perspective, the portal should be able to make real-time recommendations for related services.
ii. ☒Data captured in this environment must be obfuscated, as to not allow any party to directly target or track the preferences of an individual or their usage of the portal.
iii. ☒Solution providers should discuss in detail their use, storage, destruction of metadata, and tracking technologies with emphasis on how their offering provides analytical insights while protecting the individual user privacy.

P, N, Q, or I & Notes: N – was not described in detail and analytical insights not addressed at all.

c. Data Management

The State is seeking the ability for the portal's Constituent identity to be linked to records maintained by individual State agencies. The proposed solution will include:

- i. ☒Capabilities to streamline the sharing of data between State systems, including
  - i. The identity assurance level
  - ii. Agency to user notifications – only speaks to email notifications, what about notifying on their portal interface?
  - iii. Verification of user consent
  - iv. Identity resolution
  - v. Data sharing between agencies.
- ii. ☒Maintain a central repository of basic (core) Constituent data, that can be used by any State application to reduce data redundancy, and outdated or inaccurate information while maintaining confidentiality.
- iii. ☒Ability to integrate with State applications using, OpenID, OAuth, Web Services Federation Protocol (WS-Fed), Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), Active Directory, Application Programming Interface (API) or equivalent protocols.
- iv. ☒Ability to match the identity of the portal user to the identity of the same user in the Agency system.
- v. ☒Log all actions taken by:
  - i. Constituents
  - ii. MaineIT Support, including:
    - (a) Who made the change
    - (b) When the change was made
    - (c) What changed to and from
- vi. ☒Logging data must be available for system dashboards and reporting.

P, N, Q, or I & Notes: P

d. Customer Service

The State is seeking solution(s) to provide 24/7/365 customer service to Constituents regardless of their location or technical abilities.

- i. ☒Support Constituents with personalized and timely assistance.

    ii. ☒Provide the state options to support our Constituents across multiple channels including, but not limited to phone, email, chat, etc.

P, N, Q, or I & Notes: P

C.1. General System

a. ☒Mobile support with native app (iOS and Android)
b. ☒System availability: 24/7 with a maximum of four (4) 1-hour outages per year
c. ☒Identity relationships must be tracked in the cloud infrastructure.
d. ☒Support responsive web and web browsers.
    i. ☒Supports Windows, Chrome, and Macintosh operating systems.

P, N, Q, or I & Notes: P

C.2. ☒Compliance with MaineIT Policies & Standards

a. Architecture Compliance Policy
b. System and Services Acquisition Policy and Procedures (SA-1)
c. Application Deployment Certification Policy
d. Digital Accessibility Policy
e. Remote Hosting Policy
f. Data Exchange Policy
g. Information Security Policy
h. Access Control Policy (AC-1)
i. Access Control Procedures for Users (AC-2)
j. Risk Assessment Policy and Procedures (RA-1)
k. Vulnerability Scanning Procedure (RA-5)
l. Security Assessment and Authorization Policy and Procedures (CA-1)
m. System and Information Integrity Policy and Procedures (SI-1)
n. Configuration Management Policy (CM-1)
o. Web Standards

P, N, Q, or I & Notes: P

C.3. Support and Maintenance

a. ☒Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State’s official acceptance of the implemented solution.

P, N, Q, or I & Notes:

b. ☒Terms and duration of the support and maintenance will be specified in the contract.
P, N, Q, or I & Notes:

c. ☒All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
P, N, Q, or I & Notes:

d. ☒Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
P, N, Q, or I & Notes:

e. ☒All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
P, N, Q, or I & Notes:

f. ☒All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
P, N, Q, or I & Notes:

g. ☒User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
P, N, Q, or I & Notes: P – bidder did not offer detail but did respond yes to all

4. Security

The proposed solutions must provide a robust security system that aligns with the States Security Policies, standards, and Processes, Including:

Comply with or have the following security certifications:

i. ☐National Institute of Standards and Technology (NIST) 800-53
ii. ☐FedRamp
iii. ☐Health Insurance Portability and Accountability Act (HIPAA)
iv. ☐SOC 2 Type II
v. ☐Comply to the following security controls:
vi. ☐DDOS Protections [WN1]
vii. ☐Open Web Application Security Project (OWASP) Top 10
viii. ☐Cross Site Scripting
ix. ☐Structured Query Language (SQL) Injection

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: PruTech
DATE: 6/3/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

x. ☐Authentication bypass
xi. ☐Poorly authenticated APIs
xii. ☐Role based access controls
xiii. ☐Proper session control
xiv. ☐Real-time visibility
xv. ☐Anomalous behavior
xvi. ☐User sign with geo-location tracking
xvii. ☐Geo-blocking capabilities.
xviii. ☐Web Application Firewall [WN1]
xix. ☐System security must include the following security components:
xx. ☐Account take over protections
xxi. ☐Account sign-in Protections
xxii. ☐Behavior detection and evaluation
xxiii. ☐Adaptive AI Technology
xxiv. ☐Bot Protection; identity visitor behavior through analysis, technical and behavioral data.
xxv. ☐The proposed solution must be able to integrate with the State Security Information and Event Monitoring (SIEM) Splunk. Ability to log security information and events.

P, N, Q, or I & Notes: P – bidder responded in detail to all.

5. Licensing

☒The State is aware that multiple licensing options are available and will be required to support the proposed solution in its entirety. The State seeks bids which will provide the most cost-effective licensing approach. Bidders are required to provide a detail breakdown for the proposed licensing.

P, N, Q, or I & Notes: I – unsure if this was provided in the cost proposal, seek input during eval session.

1. Training and OCM (Organizational Change Management)

a. ☒Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution. N – bidder did not address security or identity or access management training directly. Provided technical documentation and procedural documentation/training.

b. ☒Training must include technical and administrator training, initial and ongoing as users are added.
c. ☒Continuous process to ensure Constituents that may have run into issues setting up accounts have help 24/7. N – bidder did not address
d. ☐Bidders shall guide the State in OCM engagement for the duration of project planning, transition, and final implementation phase including:
   i. Designing and managing team structures with roles and responsibilities to facilitate automated program delivery, while noting any risks anticipated from the lack of readiness in the organization and staffing.
   ii. Ensure a successful transition for the integration of new processes and technology with stakeholders.
   iii. Organizational readiness assessment

P, N, Q, or I & Notes: N – bidder did not address

3. **Disaster Recovery**
   a. ☒Availability of ninety-nine-point nine percent (99.9%) of uptime
   b. ☒Capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six (6) hours (i.e., maximum data loss cannot exceed six (6) hours)
   c. ☒Recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours.

P, N, Q, or I & Notes: P

4. **Feature Enhancements**

a. ☒The State is seeking two hundred and fifty (250) hours of time and material for each proposed technology (CIAM), Personalized Dashboard, Disclosure and Consent Management, Data Management, and Recommendation Technology) to allow for specifications and enhancements during the contract period.

P, N, Q, or I & Notes: P

5. **Project Management**
   a. ☒The State plans to have its own project manager however, the awarded Bidder must have a project manager that has the primary responsibility for executing the project management tasks associated with the project. The awarded Bidder will:

    i. Work in collaboration with the State's Project Manager - . N – bidder did not address this
    ii.
    iii. Align with State Project Management processes and practices. N – bidder did not address these two area
    iv. ☒Manage the implementation, executing all activities, tasks, deliverables and resource needs, both state and awarded Bidder. . N – bidder did not address this
  b.
  c. ☒Track project status including managing and tracking all project risks, issues and decisions.
  d. ☒Track and report status of deliverables and project status
  e. ☒The awarded Bidder will provide their approach for project management and administration services including:
    i. Project Management Methodology
    ii. Project Governance
    iii. Resource Allocation and Schedule Management approach - N
    iv. Communication Management Approach including status reporting and document repository management. - N
    v. Risk and Issue Management Methodology
    vi. Change Management Methodology
    vii. Quality Management Methodology

P, N, Q, or I & Notes: N – overall bidder did not hit all of the requirements of this section.

D. Value Added Options (Other)

☒Bidders shall provide value added optional services to address relevant matters that have not been anticipated in this RFP but contribute to successful implementation of the proposed solutions, as well as any technology or services that will reduce risk to the project's quality and continuity. The value-added technology and services will not be included in the evaluation process but may be added during the contract negotiations.

P, N, Q, or I & Notes: Nothing provided.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Servos
DATE: 6/7/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

Section I – Preliminary Information (No points – Eligibility Requirements)

(File #1 App. A, B, C)

☒Done – Pass/Fail by Procurement & RFP Coordinator

Section II Organization Qualifications and Experience

(File #2 – App. D, E + other areas that have no Appendix number but are part of File #2)

1. Overview of the Organization (App. D)

☒Bidders must include three examples of projects which demonstrate their experience and expertise in performing these services as well as highlighting the Bidder's stated qualifications and skills.

Statement of qualifications

☐Client name, contact person, Ph#, email.

Contract history with the state may be considered in rating proposals even if not provided by the bidder.

P, **N**, Q, or I & Notes:

Missing contact information; as well as which feature requirements Servos provided in their reference projects

2. Subcontractors (App. E)

☒If subcontractors are to be used, Bidders must provide the name, address, phone number, contact person, and a brief description of the subcontractors' organizational capacity and qualifications.

Business name, contact person, address, ph#, email.

P, N, Q, or I & Notes:

No subcontractors noted

3. Organizational Chart (No Appendix)

☐Bidders must provide an organizational chart. The organizational chart must include the project being proposed. Each position must be identified by position title and corresponding to the personnel job descriptions.

P, **N**, Q, or I & Notes:

No documentation provided

4. **Litigation (No App.)**
☐Bidders must attach a list of all current litigation in which the Bidder is named and a list of all closed cases that have closed within the past five (5) years in which the Bidder paid the claimant either as part of a settlement or by decree. For each, list the entity bringing suit, the complaint, the accusation, amount, and outcome.
P, **N**, Q, or **I** & Notes:
No documentation provided

5. **Financial Viability (No App.)**
☐Bidders must provide a current copy of their Dun & Bradstreet Business Information Report Snapshot.
P, **N**, Q, or **I** - Notes:
No documentation provided

6. **Licensure/Certification (No App.)**
☐Bidders *may* provide documentation of any applicable licensure/certification or specific credentials that are related to providing the proposed services of the RFP.
P, N, Q, or **I** & Notes:
N/A

7. **Certificate of Insurance (No App.)**
☐Bidders must provide a certificate of insurance on a standard ACORD form (or the equivalent) evidencing the Bidder's general liability, professional liability and any other relevant liability insurance policies that might be associated with the proposed services.
P, **N**, Q, or **I** & Notes:
No documentation provided

Section III - Proposed Services

(File #3 – App. F, G, H)

1. **Technical Assessment (App. F)**
☒Done

2. **Services to be Provided (App. G)**

Note: on App. G Detailed Technical and Functional Requirements Excel spreadsheet, a tab is labeled User Stories. No response is required for Tab 3; these were provided to bidders for clarity and understanding of the expected journey a Constituent will experience.

☒ P, Q, **N** or I Notes: Not native out of the box, need additional addons	**1. System security components System security must include the following security components:**
	1) Account Take Over Protections
	a) Account Sign-in Protections
	a) Account Sign-in Protections
	a) Adaptive AI Technology
	b) Bot Protection: identify visitor behavior through analysis of technical and behavioral data.
☒ P, Q, **N** or I Notes: Not native out of the box, need additional addons ; does not answer levels of id proofing	**2. Identity Proofing must have the ability to provide levels of proofing which will be directly tied to the constituent's level of access.**
	1) Define various levels of id proofing
	2) Document Image Capture
	3) Close coupling with authentication
☒ P, Q, **N** or I Notes: no explanation	**3. Multi-factor authentication The system must support multi-factor authentication to protect against user impersonation and credential theft.**
☐ P, Q, **N** or I	**4. Risk-based factors The system must support risk-based factors and scores that are based on factors such as, but not limited to, device and location.**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Servos
DATE: 6/7/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

Notes: no mention of location	
☒ P, Q, **N** or I Notes:	**5. Identity lifecycle management components The system must include the following identity lifecycle management components for risk-based critical applications not limited to end users but also for generic accounts and system/service accounts:**
References to requirement 2 which is an addon, but say they can provided; does not talk to articulate lifecycle clearly	1) Identity Creation
	2) Identity provisioning
	3) Attribute maps
	4) Authentication (e.g., password policies and synchronization)

☒ P, Q, **N** or I Notes: Does not talk to how	**6. Security event logging The system must log security information and events.**
	Security Information and Event Management (SIEM) – Splunk
	Cloud Services: Azure, AWS, Oracle, Google
☒ P, Q, **N** or I Notes: no supporting documentation for all certs	**7. Security Certifications The system must comply too or have the following security certifications:**

	1) NIST 800-53
	2) FedRamp
	3) HIPAA
	4) SOC 2 Type II
	Note:
	IRS require a 45-day letter approval for new cloud solutions.
☒ P, Q, **N** or I Notes: no support detail	**8. SIEM (Splunk) integration The system must be able to integrate with the State of Maine Security Information and Event Monitoring (SIEM) Splunk for Security Operations Center operations.**
☒ P, Q, **N** or I Notes: no support detail	**9. Core constituent data. The system must maintain a central repository of basic (core) constituent data, that can be used by any SoM application to reduce data redundancy and outdated or inaccurate information while maintaining confidentiality.**
☒ P, Q, **N** or I Notes: no support detail	**11. Data Management. The system must apply the Data Management Rules to the constituent profile data as per the SoM Data Management Policies.**
☒ P, Q, **N** or I Notes: no support detail	**12. SOM Employee. The system must support multiple identities for SOM employees that work with the portal in a support role.**
	1) SOM Employee identity and credentials for supporting the application.
	2) Constituent identity and credentials to use the state services offered through the portal.

☒ P, Q, **N** or I	**13. APIs. The system must be able to connect to at least one agency application.**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Servos
DATE: 6/7/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

Notes: no support detail	
	Considerations:
	a) OpenID, OAuth, WS-Fed, SAML, LDAP, Active Directory, Application Programming Interfaces (APIs), Software Development
	b) Develop once and reuse often with other agencies would be ideal
☒ P, Q, **N** or **I** Notes: no support detail	**14. User identification matching. The system must be able to match the identity of the portal user to the identity of the same user in the agency system.**
☒ P, Q, **N** or **I** Notes: no support detail	**15. Single sign-on. The system must support single sign-on to the agency application.**
☐ P, Q, **N** or **I** Notes: no support detail	**16. Import user profile data from agency systems. The system must be able to import user data from different SoM applications to ensure offboarding happens in a timely manner, so that government resources are protected from fraud. (example: death records)**
☐ P, Q, **N** or **I** Notes: no support detail	**17. History logging.** 1) The system must log all actions taken by:
	a) Constituents
	b) MaineIT support
	Including but not limited to:

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Servos
DATE: 6/7/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

	c) who made the change
	d) when the change was made
	e) what changed
☒ P, Q, **N** or **I** Notes: no support detail	**18. Reporting. The logging data (history) must be available for constituent and system dashboards and reporting in general.**
☒ P, Q, **N** or **I** Notes: nothing related to id.me	**19. Security Controls. The system must comply to the following security controls:**
	1) DDOS Protections[WN1] ,
	2) OWASP Top 10
	a) Cross Site Scripting,
	b) SQL Injection,
	3) Authentication bypass,
	a) poorly authenticated APIs,
	b) Role based access controls,
	c) proper session control
	4) Real-time visibility,
	5) Anomalous behavior,
	6) User sign with geo-location tracking,
	Geo-blocking capabilities.
	Security controls must include Web Application Firewall [WN1]
☒ P, Q, **N** or **I** Notes: no support detail	**20. General System Requirements.** 1) Mobile Support with Native App; (iOS and Android)

	2) System availability: 24/7 with 4x1-hour outages per year
	3) Identity relationships must be tracked in the cloud infrastructure.
	4) Support responsive web and web browsers.
	a. Supports Windows, Chrome, and Macintosh operating systems
☒ P, Q, **N** or I Notes: no support detail	**21. Training and Support.** 1) Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
	2) MaineIT will require technical/administrator training. There will be initial training and on-going training as users are added.
	3) Have a continuous process to ensure constituents that may have run into issues setting up accounts can have help 24/7.
☒ P, Q, **N** or I Notes: no support detail	**22. Support Requirements** 1) The Bidder will provide support, and maintenance for the solution to begin immediately after receiving the State's official acceptance of the implemented solution.
	2) Support and maintenance will be provided for the terms and duration specified in the contract.
	3) The Bidder will address all questions and reported problems related to the technical and functional operation of the system.
	4) The Bidder must provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours: 8:00 a.m. to 5:00 p.m. Eastern Standard Time.
	5) As part of the maintenance agreement, the Bidder will make all product releases and upgrades available to the State at no additional charge.
	6) All release and upgrades shall be implemented and tested by the Bidder, outside of the normal operating hours of the State government.

	7) User testing shall occur during normal State business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State government.
☒ P, Q, N or **I** Notes:	**23. Hosting** Solution can comply with MaineIT remote hosting policies. a) Remote Hosting Policy http://maine.gov/oit/policies/RemoteHostingPolicy.pdf b) Hosting Customization Policy http://maine.gov/oit/policies/HostingCustomizationPolicy.pdf
☒ P, Q, **N** or I Notes: nothing related to id.me	**24. Disaster Recovery** Proposed Solution can comply with MaineIT security requirements and remote hosting requirements, without requiring waivers, before contract finalization.
	1) Maintaining an availability metric of ninety-nine-point nine percent (99.9%) of uptime
	2) Ensuring the capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six hours (i.e., maximum data loss cannot exceed six (6) hours);
	3) Ensuring a recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours;
	4) Ensuring the hosting environment provides adequate capacity to ensure that, under ethernet connectivity to the client device, data inquiry/lookup response is within three (3) seconds, and data modification response is within five (5) seconds;
	5) Providing the Department at least thirty (30) calendar day advance written notice of any material change in network operations or architecture;
	6) Ensuring any planned material change in network operations or architecture cannot be made without the prior written consent of the Department; and Outlining of all Service Level Agreements (SLAs) for technical support (the awarded Bidder shall be open to negotiation to ensure the SLAs meet the Department’s needs

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Servos
DATE: 6/7/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

☒1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
P, N, Q, or **I** & Notes: why is sso listed as future goal?

☒1b) Detailed description of the technologies, software and / or hardware for each of the components.
P, N, Q, or **I** & Notes:

☒1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.
P, N, Q, or **I** & Notes:

☒1d) Description of the overall platform and architecture of the proposed solution(s).
P, N, Q, or **I** & Notes:
Lacking a visual for architecture

☒1e) Description of any third-party software or partnerships required for the proposed Solution(s).
P, N, Q, or **I** & Notes:

☒2a) A detailed timeline and description of milestones, deliverables, tasks
P, N, Q, or **I** & Notes:

☒2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period
P, **N**, Q, or I & Notes:
Does not talk to post implementation support or state side resourcing

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Servos
DATE: 6/7/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

☒2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
P, N, Q, or I & Notes:

☒2d) Average time to market for each component.
P, N, Q, or I & Notes:

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. ☒Capture Constituent Identity and profile data.
   P, N, Q, or I & Notes:
b. ☒Provide identity provisioning and deprovisioning.
   P, **N**, Q, or I & Notes: does not talk to deprovisioning
c. ☒Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
   i. Identity Creation
   ii. Identity provisioning
   iii. Attribute maps
   iv. Authentication (e.g., password policies and synchronization)
      P, **N**, Q, or I & Notes: does not talk to attribute map
d. ☒Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies.
   P, **N**, Q, or I & Notes: doesn't talk where in the flow of the CP idme is located or how with servicenow/idme/som applications work together
e. ☒Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
   P, **N**, Q, or I & Notes: doesn't talk to integration with auth sources
f. ☒Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.
   P, N, Q, or **I** & Notes:

g. ☐Allow for multiple role selections for the following identities:
  i. Individual
  ii. Business Owner
  iii. Support multiple identities for State employees that work with the portal in a support role:
    (a) SOM Employee identity and credentials for supporting the application.
    (b) Constituent identity and credentials to use the state services offered through the portal.
  iv. Multi role individual (Individual and Business Owner)
  P, **N**, Q, or I & Notes: doesn't talk to these requirements

h. ☒Have the ability to provide levels of proofing which will be directly tied to the Constituent's level of consent given.
P, **N**, Q, or I & Notes: not mentioned

i. ☒Support multi-factor authentication to protect against user impersonation and credential theft.
P, N, Q, or **I** & Notes:

B.2. ☒The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.
P, N, Q, or **I** & Notes:

a. Disclosure and Consent Management

The desire of the State is to be as transparent as possible and respect the privacy of the individual interacting with the Constituents' Portal. Consent is a core tenant of maintaining the public trust in the Constituents' Portal and will be a foundational component of the architecture.

The Disclosure and Consent Management solution shall include:

  i. ☐Granular consent management that encompasses the automated functions necessary to create, modify, revoke, and manage Constituent consents.

ii. ☐Allow users the ability to opt-in and opt-out of data sharing and services within the Constituents' portal.
iii. ☒Obtain user consent both in an interactive and set preference mode for a variety of transactions on the Portal.
iv. ☒Support administrative users' management of standard legal disclaimers and data classification for transactions.
v. ☐Highly configurable with version control and history tracking for consent language.
vi. ☒Ability for end user to access a retrievable log of granted consent and data usage on the portal derived from the consent.

P, N, Q, or **I** & Notes:

b. Recommendation Technology

The State is seeking options which, while maintaining individual privacy, will collect and analyze data about user interactions, behavior, and preferences. The expected outcome of this will be to provide insights and intelligence that help the State make informed decisions and improve Constituent experiences.

i. ☒From the user perspective, the portal should be able to make real-time recommendations for related services.
ii. ☐Data captured in this environment must be obfuscated, as to not allow any party to directly target or track the preferences of an individual or their usage of the portal.
iii. ☒Solution providers should discuss in detail their use, storage, destruction of metadata, and tracking technologies with emphasis on how their offering provides analytical insights while protecting the individual user privacy.

P, **N**, Q, or I & Notes:
It sounds possible but to be affective it needs non obfuscated data

c. Data Management

The State is seeking the ability for the portal's Constituent identity to be linked to records maintained by individual State agencies. The proposed solution will include:

i. ☐Capabilities to streamline the sharing of data between State systems, including
    i. The identity assurance level

        ii. Agency to user notifications
        iii. Verification of user consent
        iv. Identity resolution
        v. Data sharing between agencies.
    ii. ☒Maintain a central repository of basic (core) Constituent data, that can be used by any State application to reduce data redundancy, and outdated or inaccurate information while maintaining confidentiality.
    iii. ☒Ability to integrate with State applications using, OpenID, OAuth, Web Services Federation Protocol (WS-Fed), Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), Active Directory, Application Programming Interface (API) or equivalent protocols.
    iv. ☐Ability to match the identity of the portal user to the identity of the same user in the Agency system.
    v. ☒Log all actions taken by:
        i. Constituents
        ii. MaineIT Support, including:
            (a) Who made the change
            (b) When the change was made
            (c) What changed to and from
    vi. ☒Logging data must be available for system dashboards and reporting.

P, **N**, Q, or I & Notes:

Does not meet all requirements; concerns around core being a cmdb

d. Customer Service

The State is seeking solution(s) to provide 24/7/365 customer service to Constituents regardless of their location or technical abilities.

    i. ☐Support Constituents with personalized and timely assistance.
    ii. ☒Provide the state options to support our Constituents across multiple channels including, but not limited to phone, email, chat, etc.

P, **N,** Q, or I & Notes:

Does not cover all features of solution; no mention idme

C.1. General System

a. ☐Mobile support with native app (iOS and Android)
b. ☐System availability: 24/7 with a maximum of four (4) 1-hour outages per year
c. ☐Identity relationships must be tracked in the cloud infrastructure.
d. ☒Support responsive web and web browsers.

i. ☒Supports Windows, Chrome, and Macintosh operating systems.

P, **N**, Q, or I & Notes:
Does not meet uptime requirements or talk to all parts of the solution

C.2. ☒Compliance with MaineIT Policies & Standards

a. Architecture Compliance Policy
b. System and Services Acquisition Policy and Procedures (SA-1)
c. Application Deployment Certification Policy
d. Digital Accessibility Policy
e. Remote Hosting Policy
f. Data Exchange Policy
g. Information Security Policy
h. Access Control Policy (AC-1)
i. Access Control Procedures for Users (AC-2)
j. Risk Assessment Policy and Procedures (RA-1)
k. Vulnerability Scanning Procedure (RA-5)
l. Security Assessment and Authorization Policy and Procedures (CA-1)
m. System and Information Integrity Policy and Procedures (SI-1)
n. Configuration Management Policy (CM-1)
o. Web Standards

P, N, Q, or **I** & Notes:

C.3. Support and Maintenance

a. ☒Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State's official acceptance of the implemented solution.
P, N, Q, or **I** & Notes:
b. ☒Terms and duration of the support and maintenance will be specified in the contract.
P, N, Q, or **I** & Notes:

c. ☒All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
P, N, Q, or **I** & Notes:
d. ☐Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the

approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
P, **N**, Q, or I & Notes: no metion of toll free number

e. ☒All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
P, N, Q, or **I** & Notes:

f. ☒All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
P, N, Q, or **I** & Notes:

g. ☒User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
P, N, Q, or **I** & Notes:

4. Security

The proposed solutions must provide a robust security system that aligns with the States Security Policies, standards, and Processes, Including:

Comply with or have the following security certifications:

i. ☐National Institute of Standards and Technology (NIST) 800-53
ii. ☐FedRamp
iii. ☐Health Insurance Portability and Accountability Act (HIPAA)
iv. ☐SOC 2 Type II
v. ☐Comply to the following security controls:
vi. ☐DDOS Protections [WN1]
vii. ☐Open Web Application Security Project (OWASP) Top 10
viii. ☐Cross Site Scripting
ix. ☐Structured Query Language (SQL) Injection
x. ☐Authentication bypass
xi. ☐Poorly authenticated APIs
xii. ☐Role based access controls
xiii. ☐Proper session control
xiv. ☐Real-time visibility
xv. ☐Anomalous behavior
xvi. ☐User sign with geo-location tracking
xvii. ☐Geo-blocking capabilities.
xviii. ☐Web Application Firewall [WN1]

xix. ☐System security must include the following security components:
xx. ☐Account take over protections
xxi. ☐Account sign-in Protections
xxii. ☐Behavior detection and evaluation
xxiii. ☐Adaptive AI Technology
xxiv. ☐Bot Protection; identity visitor behavior through analysis, technical and behavioral data.
xxv. ☐The proposed solution must be able to integrate with the State Security Information and Event Monitoring (SIEM) Splunk. Ability to log security information and events.

P, **N**, Q, or I & Notes:
talks only to servicenow and not full solution

5. Licensing

☒The State is aware that multiple licensing options are available and will be required to support the proposed solution in its entirety. The State seeks bids which will provide the most cost-effective licensing approach. Bidders are required to provide a detail breakdown for the proposed licensing.

P, **N**, Q, or I & Notes:
no licensing documentation provided

1. Training and OCM (Organizational Change Management)

a. ☒Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
b. ☒Training must include technical and administrator training, initial and ongoing as users are added.
c. ☒Continuous process to ensure Constituents that may have run into issues setting up accounts have help 24/7.
d. ☒Bidders shall guide the State in OCM engagement for the duration of project planning, transition, and final implementation phase including:
    i. Designing and managing team structures with roles and responsibilities to facilitate automated program delivery, while noting any risks anticipated from the lack of readiness in the organization and staffing.
    ii. Ensure a successful transition for the integration of new processes and technology with stakeholders.
    iii. Organizational readiness assessment

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Servos
DATE: 6/7/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

P, N, Q, or **I** & Notes:

3. Disaster Recovery

a. ☐Availability of ninety-nine-point nine percent (99.9%) of uptime
b. ☐Capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six (6) hours (i.e., maximum data loss cannot exceed six (6) hours)
c. ☐Recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours.

P, **N**, Q, or I & Notes:
Does not meet requirements

4. Feature Enhancements

a. ☐The State is seeking two hundred and fifty (250) hours of time and material for each proposed technology (CIAM), Personalized Dashboard, Disclosure and Consent Management, Data Management, and Recommendation Technology) to allow for specifications and enhancements during the contract period.

P, **N**, Q, or I & Notes:
Does not meet requirement

5. Project Management

a. ☐The State plans to have its own project manager however, the awarded Bidder must have a project manager that has the primary responsibility for executing the project management tasks associated with the project. The awarded Bidder will:
    i. Work in collaboration with the State's Project Manager
    ii. Align with State Project Management processes and practices.
b. ☒Manage the implementation, executing all activities, tasks, deliverables and resource needs, both state and awarded Bidder.
c. ☒Track project status including managing and tracking all project risks, issues and decisions.
d. ☒Track and report status of deliverables and project status
e. ☐The awarded Bidder will provide their approach for project management and administration services including:
    i. Project Management Methodology
    ii. Project Governance

iii. Resource Allocation and Schedule Management approach
iv. Communication Management Approach including status reporting and document repository management.
v. Risk and Issue Management Methodology
vi. Change Management Methodology
vii. Quality Management Methodology

P, **N**, Q, or I & Notes:

Does not cover all requirements

D. Value Added Options (Other)

☒Bidders shall provide value added optional services to address relevant matters that have not been anticipated in this RFP but contribute to successful implementation of the proposed solutions, as well as any technology or services that will reduce risk to the project's quality and continuity. The value-added technology and services will not be included in the evaluation process but may be added during the contract negotiations.

P, N, Q, or **I** & Notes:

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Servos
DATE: 05 June 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: MaineIT

Section I – Preliminary Information (No points – Eligibility Requirements)

(File #1 App. A, B, C)

☒Done – Pass/Fail by Procurement & RFP Coordinator

Section II Organization Qualifications and Experience

(File #2 – App. D, E + other areas that have no Appendix number but are part of File #2)

1. **Overview of the Organization (App. D)**
   ☒Bidders must include three examples of projects which demonstrate their experience and expertise in performing these services as well as highlighting the Bidder's stated qualifications and skills.
   P: Adequate response
   Q: Four examples, instead of three

   Statement of qualifications
   ☒Client name, contact person, Ph#, email.
   Contract history with the state may be considered in rating proposals even if not provided by the bidder.
   P: Strong response

2. **Subcontractors (App. E)**
   ☒If subcontractors are to be used, Bidders must provide the name, address, phone number, contact person, and a brief description of the subcontractors' organizational capacity and qualifications.
   Business name, contact person, address, ph#, email.
   P: No subcontractor

3. **Organizational Chart (No Appendix)**
   ☐Bidders must provide an organizational chart. The organizational chart must include the project being proposed. Each position must be identified by position title and corresponding to the personnel job descriptions.
   N: NO response

4. **Litigation (No App.)**
   ☐Bidders must attach a list of all current litigation in which the Bidder is named and a list of all closed cases that have closed within the past five (5) years in which the

Bidder paid the claimant either as part of a settlement or by decree. For each, list the entity bringing suit, the complaint, the accusation, amount, and outcome.
N: NO response

5. **Financial Viability (No App.)**
☐Bidders must provide a current copy of their Dun & Bradstreet Business Information Report Snapshot.
N: NO response

6. **Licensure/Certification (No App.)**
☐Bidders *may* provide documentation of any applicable licensure/certification or specific credentials that are related to providing the proposed services of the RFP.
N: NO response

7. **Certificate of Insurance (No App.)**
☒Bidders must provide a certificate of insurance on a standard ACORD form (or the equivalent) evidencing the Bidder's general liability, professional liability and any other relevant liability insurance policies that might be associated with the proposed services.
N: NO response

Section III - Proposed Services

(File #3 – App. F, G, H)

1. **Technical Assessment (App. F)**
☒Done

2. **Services to be Provided (App. G)**

Note: on App. G Detailed Technical and Functional Requirements Excel spreadsheet, a tab is labeled User Stories. No response is required for Tab 3; these were provided to bidders for clarity and understanding of the expected journey a Constituent will experience.

☒ *P: Weak response (Covers ID.me, but NOT ServiceNow)*	1. **System security components System security must include the following security components:**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Servos
DATE: 05 June 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: MaineIT

Q: Was the Add-On accommodated in the Cost Form?	
	1) Account Take Over Protections
	a) Account Sign-in Protections
	a) Account Sign-in Protections
	a) Adaptive AI Technology
	b) Bot Protection: identify visitor behavior through analysis of technical and behavioral data.
☒ *P: Strong response for #1 & #2* *N: Weak response for #3* *Q: Was the Add-On accommodated in the Cost Form?*	**2. Identity Proofing must have the ability to provide levels of proofing which will be directly tied to the constituent's level of access.**
	1) Define various levels of id proofing
	2) Document Image Capture
	3) Close coupling with authentication
☒ *N: Weak response (No explanation)*	**3. Multi-factor authentication The system must support multi-factor authentication to protect against user impersonation and credential theft.**
☒ *N: Weak response (Covers ID.me, but NOT ServiceNow)* *N: No explanation of the Partial*	**4. Risk-based factors The system must support risk-based factors and scores that are based on factors such as, but not limited to, device and location.**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Servos
DATE: 05 June 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: MaineIT

☒ *P: Weak response (Covers ID.me, but NOT ServiceNow)*	**5. Identity lifecycle management components The system must include the following identity lifecycle management components for risk-based critical applications not limited to end users but also for generic accounts and system/service accounts:**
	1) Identity Creation
	2) Identity provisioning
	3) Attribute maps
	4) Authentication (e.g., password policies and synchronization)
☒ *N: Weak response. No explanation.*	**6. Security event logging The system must log security information and events.**
	Security Information and Event Management (SIEM) – Splunk
	Cloud Services: Azure, AWS, Oracle, Google
☒ *N: Weak response (Covers ServiceNow, but NOT ID.me)* *N: Did NOT ack the IRS 45-day notice*	**7. Security Certifications The system must comply too or have the following security certifications:**
	1) NIST 800-53
	2) FedRamp
	3) HIPAA
	4) SOC 2 Type II
	Note:
	IRS require a 45-day letter approval for new cloud solutions.

☒ *N: Weak response. No explanation.*	**8. SIEM (Splunk) integration The system must be able to integrate with the State of Maine Security Information and Event Monitoring (SIEM) Splunk for Security Operations Center operations.**
☒ *N: Weak response. No explanation.*	**9. Core constituent data. The system must maintain a central repository of basic (core) constituent data, that can be used by any SoM application to reduce data redundancy and outdated or inaccurate information while maintaining confidentiality.**
☒ *N: Weak response. No explanation.*	**11. Data Management. The system must apply the Data Management Rules to the constituent profile data as per the SoM Data Management Policies.**
☒ *N: Weak response. No explanation.*	**12. SOM Employee. The system must support multiple identities for SOM employees that work with the portal in a support role.**
	1) SOM Employee identity and credentials for supporting the application.
	2) Constituent identity and credentials to use the state services offered through the portal.
☒ *N: Weak response. No explanation.*	**13. APIs. The system must be able to connect to at least one agency application.**
	Considerations:
	a) OpenID, OAuth, WS-Fed, SAML, LDAP, Active Directory, Application Programming Interfaces (APIs), Software Development
	b) Develop once and reuse often with other agencies would be ideal
☒ *N: Weak response. No explanation.*	**14. User identification matching. The system must be able to match the identity of the portal user to the identity of the same user in the agency system.**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Servos
DATE: 05 June 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: MaineIT

☒ *N: Weak response. No explanation.*	**15. Single sign-on. The system must support single sign-on to the agency application.**
☒ *N: Weak response. No explanation.*	**16. Import user profile data from agency systems. The system must be able to import user data from different SoM applications to ensure offboarding happens in a timely manner, so that government resources are protected from fraud. (example: death records)**
☒ *N: Weak response. No explanation.*	**17. History logging.** 1) The system must log all actions taken by:
	a) Constituents
	b) MaineIT support
	Including but not limited to:
	c) who made the change
	d) when the change was made
	e) what changed
☒ *N: Weak response. No explanation.*	**18. Reporting. The logging data (history) must be available for constituent and system dashboards and reporting in general.**
☒ *N: Weak response (Covers ServiceNow, but NOT ID.me)*	**19. Security Controls. The system must comply to the following security controls:**
	1) DDOS Protections[WN1] ,
	2) OWASP Top 10
	a) Cross Site Scripting,
	b) SQL Injection,
	3) Authentication bypass,
	a) poorly authenticated APIs,
	b) Role based access controls,

	c) proper session control
	4) Real-time visibility,
	5) Anomalous behavior,
	6) User sign with geo-location tracking,
	Geo-blocking capabilities.
	Security controls must include Web Application Firewall [WN1]
☒ *N: Weak response. No explanation.*	**20. General System Requirements.** 1) Mobile Support with Native App; (iOS and Android)
	2) System availability: 24/7 with 4x1-hour outages per year
	3) Identity relationships must be tracked in the cloud infrastructure.
	4) Support responsive web and web browsers.
	a. Supports Windows, Chrome, and Macintosh operating systems
☒ *N: Weak response. No explanation.*	**21. Training and Support.** 1) Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
	2) MaineIT will require technical/administrator training. There will be initial training and on-going training as users are added.
	3) Have a continuous process to ensure constituents that may have run into issues setting up accounts can have help 24/7.
☒ *N: Weak response. No explanation.*	**22. Support Requirements** 1) The Bidder will provide support, and maintenance for the solution to begin immediately after receiving the State's official acceptance of the implemented solution.
	2) Support and maintenance will be provided for the terms and duration specified in the contract.
	3) The Bidder will address all questions and reported problems related to the technical and functional operation of the system.
	4) The Bidder must provide toll-free telephone support through a qualified technician with direct and demonstrated

	experience in the implementation and maintenance of the approved implemented solution during regular business hours: 8:00 a.m. to 5:00 p.m. Eastern Standard Time.
	5) As part of the maintenance agreement, the Bidder will make all product releases and upgrades available to the State at no additional charge.
	6) All release and upgrades shall be implemented and tested by the Bidder, outside of the normal operating hours of the State government.
	7) User testing shall occur during normal State business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State government.
☒ *N: Weak response. Irrelevant explanation.*	**23. Hosting** Solution can comply with MaineIT remote hosting policies. a) Remote Hosting Policy http://maine.gov/oit/policies/RemoteHostingPolicy.pdf b) Hosting Customization Policy http://maine.gov/oit/policies/HostingCustomizationPolicy.pdf
☒ *N: Weak response (Covers ServiceNow, but NOT ID.me)*	**24. Disaster Recovery** Proposed Solution can comply with MaineIT security requirements and remote hosting requirements, without requiring waivers, before contract finalization.
	1) Maintaining an availability metric of ninety-nine-point nine percent (99.9%) of uptime
	2) Ensuring the capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six hours (i.e., maximum data loss cannot exceed six (6) hours);
	3) Ensuring a recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours;
	4) Ensuring the hosting environment provides adequate capacity to ensure that, under ethernet connectivity to the client device, data inquiry/lookup response is within three (3) seconds, and data modification response is within five (5) seconds;

	5) Providing the Department at least thirty (30) calendar day advance written notice of any material change in network operations or architecture;
	6) Ensuring any planned material change in network operations or architecture cannot be made without the prior written consent of the Department; and Outlining of all Service Level Agreements (SLAs) for technical support (the awarded Bidder shall be open to negotiation to ensure the SLAs meet the Department's needs

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

☒1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
P: Strong response

☒1b) Detailed description of the technologies, software and / or hardware for each of the components.
P: Strong response

☒1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.
P: Strong response

☒1d) Description of the overall platform and architecture of the proposed solution(s).
P: Strong response

☒1e) Description of any third-party software or partnerships required for the proposed Solution(s).
P: Strong response

☒2a) A detailed timeline and description of milestones, deliverables, tasks
P: Weak response. Does include a basic timeline, but NO milestones, or deliverables, or tasks.

☒2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through

Implementation Period and Post Implementation – Support period
P: Adequate response

☒2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
P: Adequate response

☒2d) Average time to market for each component.
P: Adequate response

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. ☒Capture Constituent Identity and profile data.
N: Red flag! Above, in 1a & 1b, the bidder states that Identity Provisioning (Authentication) is handled by ServiceNow, whereas in this item, the statement is that ID.me is going to manage Identity Provisioning (Authentication). This is a fundamental inconsistency. (All sections are consistent that ID.me provides Identity Proofing.)

b. ☒Provide identity provisioning and deprovisioning.
N: Red flag! It is all about ID.me, as opposed to earlier statement re: ServiceNow.

c. ☒Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
    i. Identity Creation
    ii. Identity provisioning
    iii. Attribute maps
    iv. Authentication (e.g., password policies and synchronization)
    N: Red flag! It is all about ID.me, as opposed to earlier statement re: ServiceNow.

d. ☒Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods

currently utilized by State Agencies.
N: Red flag! It is all about ID.me, as opposed to earlier statement re: ServiceNow.

e. ☒Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
N: Irrelevant response

f. ☒Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.
N: Does not directly respond

g. ☒Allow for multiple role selections for the following identities:
  i. Individual
  ii. Business Owner
  iii. Support multiple identities for State employees that work with the portal in a support role:
    (a) SOM Employee identity and credentials for supporting the application.
    (b) Constituent identity and credentials to use the state services offered through the portal.
  iv. Multi role individual (Individual and Business Owner)
N: Red flag! It is all about ID.me, as opposed to earlier statement re: ServiceNow.

h. ☒Have the ability to provide levels of proofing which will be directly tied to the Constituent's level of consent given.
P: Adequate response

i. ☒Support multi-factor authentication to protect against user impersonation and credential theft.
N: Red flag! It is all about ID.me, as opposed to earlier statement re: ServiceNow.

B.2. ☒The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find

State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.
P: Adequate response

a. Disclosure and Consent Management
The desire of the State is to be as transparent as possible and respect the privacy of the individual interacting with the Constituents' Portal. Consent is a core tenant of maintaining the public trust in the Constituents' Portal and will be a foundational component of the architecture.
The Disclosure and Consent Management solution shall include:

i. ☒Granular consent management that encompasses the automated functions necessary to create, modify, revoke, and manage Constituent consents.
P: Adequate response

ii. ☒Allow users the ability to opt-in and opt-out of data sharing and services within the Constituents' portal.
P: Adequate response

iii. ☒Obtain user consent both in an interactive and set preference mode for a variety of transactions on the Portal.
N: Weak response. Only interactive is available, as opposed to set preference mode.

iv. ☒Support administrative users' management of standard legal disclaimers and data classification for transactions.
N: Weak response. Legal disclaimers could be accommodated via URLs, but it would require admin assistance for any change. No mention of data classification.

v. ☒Highly configurable with version control and history tracking for consent language.
N: No version control history

vi. ☒Ability for end user to access a retrievable log of granted consent and data usage on the portal derived from the consent.
P: Adequate response

b. Recommendation Technology

The State is seeking options which, while maintaining individual privacy, will collect and analyze data about user interactions, behavior, and preferences. The expected outcome of this will be to provide insights and intelligence that help the State make informed decisions and improve Constituent experiences.

i. ☒From the user perspective, the portal should be able to make real-time recommendations for related services.
P: Adequate response

ii. ☒Data captured in this environment must be obfuscated, as to not allow any party to directly target or track the preferences of an individual or their usage of the portal.
N: Weak response

iii. ☒Solution providers should discuss in detail their use, storage, destruction of metadata, and tracking technologies with emphasis on how their offering provides analytical insights while protecting the individual user privacy.
N: Irrelevant response

c. Data Management

The State is seeking the ability for the portal's Constituent identity to be linked to records maintained by individual State agencies. The proposed solution will include:

i. ☒Capabilities to streamline the sharing of data between State systems, including
   i. The identity assurance level
   ii. Agency to user notifications
   iii. Verification of user consent
   iv. Identity resolution
   v. Data sharing between agencies.

   P: Adequate response
   N: Unclear of the division-of-labor between ServiceNow & ID.me

ii. ☒Maintain a central repository of basic (core) Constituent data, that can be used by any State application to reduce data redundancy, and outdated or inaccurate information while maintaining confidentiality.
P: Adequate response
N: Unclear of the division-of-labor between ServiceNow & ID.me

iii. ☒Ability to integrate with State applications using, OpenID, OAuth, Web Services Federation Protocol (WS-Fed), Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), Active Directory, Application Programming Interface (API) or equivalent protocols.
P: Adequate response
N: Unclear of the division-of-labor between ServiceNow & ID.me

iv. ☒Ability to match the identity of the portal user to the identity of the same user in the Agency system.
N: No response

v. ☒Log all actions taken by:
  i. Constituents
  ii. MaineIT Support, including:
    (a) Who made the change
    (b) When the change was made
    (c) What changed to and from
N: No response

vi. ☒Logging data must be available for system dashboards and reporting.
N: No response

d. Customer Service
The State is seeking solution(s) to provide 24/7/365 customer service to Constituents regardless of their location or technical abilities.
  i. ☒Support Constituents with personalized and timely assistance.
  ii. ☒Provide the state options to support our Constituents across multiple channels including, but not limited to phone, email, chat, etc.
Q: Was it included in the Cost Proposal?
N: Weak response. Covers ServiceNow, but NOT ID.me.

C.1. General System
  a. ☒Mobile support with native app (iOS and Android)
  b. ☒System availability: 24/7 with a maximum of four (4) 1-hour outages per year
  c. ☒Identity relationships must be tracked in the cloud infrastructure.
  d. ☒Support responsive web and web browsers.

i. ☒Supports Windows, Chrome, and Macintosh operating systems.

N: Weak response. Covers ServiceNow, but NOT ID.me.

C.2. ☒Compliance with MaineIT Policies & Standards

a. Architecture Compliance Policy
b. System and Services Acquisition Policy and Procedures (SA-1)
c. Application Deployment Certification Policy
d. Digital Accessibility Policy
e. Remote Hosting Policy
f. Data Exchange Policy
g. Information Security Policy
h. Access Control Policy (AC-1)
i. Access Control Procedures for Users (AC-2)
j. Risk Assessment Policy and Procedures (RA-1)
k. Vulnerability Scanning Procedure (RA-5)
l. Security Assessment and Authorization Policy and Procedures (CA-1)
m. System and Information Integrity Policy and Procedures (SI-1)
n. Configuration Management Policy (CM-1)
o. Web Standards

N: Weak response. Covers ServiceNow, but NOT ID.me.

C.3. Support and Maintenance

a. ☒Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State's official acceptance of the implemented solution.
N: Weak response. Covers ServiceNow, but NOT ID.me.

b. ☒Terms and duration of the support and maintenance will be specified in the contract.
N: Weak response. Covers ServiceNow, but NOT ID.me.

c. ☒All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
N: Weak response. Covers ServiceNow, but NOT ID.me.

d. ☒Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)

N: Weak response. Covers ServiceNow, but NOT ID.me.

e. ☒All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
N: Weak response. Covers ServiceNow, but NOT ID.me.

f. ☐All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
N: No response

g. ☐User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
N: No response

4. Security

The proposed solutions must provide a robust security system that aligns with the States Security Policies, standards, and Processes, Including:

Comply with or have the following security certifications:

i. ☐National Institute of Standards and Technology (NIST) 800-53
ii. ☐FedRamp
iii. ☐Health Insurance Portability and Accountability Act (HIPAA)
iv. ☐SOC 2 Type II
v. ☐Comply to the following security controls:
vi. ☐DDOS Protections [WN1]
vii. ☐Open Web Application Security Project (OWASP) Top 10
viii. ☐Cross Site Scripting
ix. ☐Structured Query Language (SQL) Injection
x. ☐Authentication bypass
xi. ☐Poorly authenticated APIs
xii. ☐Role based access controls
xiii. ☐Proper session control
xiv. ☐Real-time visibility
xv. ☐Anomalous behavior
xvi. ☐User sign with geo-location tracking
xvii. ☐Geo-blocking capabilities.
xviii. ☐Web Application Firewall [WN1]

xix. ☐System security must include the following security components:
xx. ☐Account take over protections
xxi. ☐Account sign-in Protections
xxii. ☐Behavior detection and evaluation
xxiii. ☐Adaptive AI Technology
xxiv. ☐Bot Protection; identity visitor behavior through analysis, technical and behavioral data.
xxv. ☐The proposed solution must be able to integrate with the State Security Information and Event Monitoring (SIEM) Splunk. Ability to log security information and events.

N: Generic response. Does NOT cover the specifics.
N: Weak response. Covers ServiceNow, but NOT ID.me.

5. Licensing

☒The State is aware that multiple licensing options are available and will be required to support the proposed solution in its entirety. The State seeks bids which will provide the most cost-effective licensing approach. Bidders are required to provide a detail breakdown for the proposed licensing.

Q: What is Appendix I? Is that the Cost Form?

1. Training and OCM (Organizational Change Management)

a. ☐Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
b. ☐Training must include technical and administrator training, initial and ongoing as users are added.
c. ☐Continuous process to ensure Constituents that may have run into issues setting up accounts have help 24/7.
d. ☐Bidders shall guide the State in OCM engagement for the duration of project planning, transition, and final implementation phase including:
    i. Designing and managing team structures with roles and responsibilities to facilitate automated program delivery, while noting any risks anticipated from the lack of readiness in the organization and staffing.
    ii. Ensure a successful transition for the integration of new processes and technology with stakeholders.
    iii. Organizational readiness assessment

N: Generic boilerplate response. Did NOT address any specifics.

3. **Disaster Recovery**
   a. ☒Availability of ninety-nine-point nine percent (99.9%) of uptime
   b. ☒Capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six (6) hours (i.e., maximum data loss cannot exceed six (6) hours)
   c. ☒Recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours.

   N: Generic boilerplate response. Did NOT address specifics.
   N: Covers ServiceNow, NOT ID.me.

4. **Feature Enhancements**

a. ☒The State is seeking two hundred and fifty (250) hours of time and material for each proposed technology (CIAM), Personalized Dashboard, Disclosure and Consent Management, Data Management, and Recommendation Technology) to allow for specifications and enhancements during the contract period.
   P: Irrelevant response

5. **Project Management**
   a. ☒The State plans to have its own project manager however, the awarded Bidder must have a project manager that has the primary responsibility for executing the project management tasks associated with the project. The awarded Bidder will:
      i. Work in collaboration with the State's Project Manager
      ii. Align with State Project Management processes and practices.
   b. ☒Manage the implementation, executing all activities, tasks, deliverables and resource needs, both state and awarded Bidder.
   c. ☒Track project status including managing and tracking all project risks, issues and decisions.
   d. ☒Track and report status of deliverables and project status
   e. ☒The awarded Bidder will provide their approach for project management and administration services including:
      i. Project Management Methodology
      ii. Project Governance
      iii. Resource Allocation and Schedule Management approach
      iv. Communication Management Approach including status reporting and document repository management.
      v. Risk and Issue Management Methodology
      vi. Change Management Methodology

vii. Quality Management Methodology
N: Weak response overall

D. Value Added Options (Other)

☒Bidders shall provide value added optional services to address relevant matters that have not been anticipated in this RFP but contribute to successful implementation of the proposed solutions, as well as any technology or services that will reduce risk to the project's quality and continuity. The value-added technology and services will not be included in the evaluation process but may be added during the contract negotiations.
P: Adequate response

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Servos
DATE: 5/23/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

Section I – Preliminary Information (No points – Eligibility Requirements)

(File #1 App. A, B, C)

☒Done – Pass/Fail by Procurement & RFP Coordinator

Section II Organization Qualifications and Experience

(File #2 – App. D, E + other areas that have no Appendix number but are part of File #2)

1. **Overview of the Organization (App. D)**
   ☒Bidders must include three examples of projects which demonstrate their experience and expertise in performing these services as well as highlighting the Bidder's stated qualifications and skills.

   Statement of qualifications
   ☒Client name, contact person, Ph#, email.
   Contract history with the state may be considered in rating proposals even if not provided by the bidder.

   P, N, Q, or I & Notes: P

2. **Subcontractors (App. E)**
   ☒If subcontractors are to be used, Bidders must provide the name, address, phone number, contact person, and a brief description of the subcontractors' organizational capacity and qualifications.
   Business name, contact person, address, ph#, email.
   P, N, Q, or I & Notes: No subcontractors listed.

3. **Organizational Chart (No Appendix)**
   ☒Bidders must provide an organizational chart. The organizational chart must include the project being proposed. Each position must be identified by position title and corresponding to the personnel job descriptions.
   P, N, Q, or I & Notes: N – org chart not provided

4. **Litigation (No App.)**

☒Bidders must attach a list of all current litigation in which the Bidder is named and a list of all closed cases that have closed within the past five (5) years in which the Bidder paid the claimant either as part of a settlement or by decree. For each, list the entity bringing suit, the complaint, the accusation, amount, and outcome.
P, N, Q, or I & Notes: N-not provided

5. **Financial Viability (No App.)**
☐Bidders must provide a current copy of their Dun & Bradstreet Business Information Report Snapshot.
P, N, Q, or I - Notes: N – not provided

6. **Licensure/Certification (No App.)**
☒Bidders *may* provide documentation of any applicable licensure/certification or specific credentials that are related to providing the proposed services of the RFP.
P, N, Q, or I & Notes: N – not provided

7. **Certificate of Insurance (No App.)**
☒Bidders must provide a certificate of insurance on a standard ACORD form (or the equivalent) evidencing the Bidder's general liability, professional liability and any other relevant liability insurance policies that might be associated with the proposed services.
P, N, Q, or I & Notes: N – not provided

Section III - Proposed Services

(File #3 – App. F, G, H)

1. **Technical Assessment (App. F)**
☒Done

2. **Services to be Provided (App. G)**

Note: on App. G Detailed Technical and Functional Requirements Excel spreadsheet, a tab is labeled User Stories. No response is required for Tab 3; these were provided to bidders for clarity and understanding of the expected journey a Constituent will experience.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Servos
DATE: 5/23/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes: P does not mention BOT protection by name.	**1. System security components System security must include the following security components:**
	1) Account Take Over Protections
	a) Account Sign-in Protections
	a) Account Sign-in Protections
	a) Adaptive AI Technology
	b) Bot Protection: identify visitor behavior through analysis of technical and behavioral data.
☒ P, Q, N or I Notes: Q – I am unsure if the proofing addresses the document image capture, could not make that assumption when reading the description.	**2. Identity Proofing must have the ability to provide levels of proofing which will be directly tied to the constituent's level of access.**
	1) Define various levels of id proofing
	2) Document Image Capture
	3) Close coupling with authentication
☒ P, Q, N or I Notes: P- they did not describe it but it was listed in statements above.	**3. Multi-factor authentication The system must support multi-factor authentication to protect against user impersonation and credential theft.**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Servos
DATE: 5/23/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes: Q – I was not able to tell if this was an adequate response for the bidders “Partial”	**4. Risk-based factors The system must support risk-based factors and scores that are based on factors such as, but not limited to, device and location.**
☒ P, Q, N or I Notes: Q	**5. Identity lifecycle management components The system must include the following identity lifecycle management components for risk-based critical applications not limited to end users but also for generic accounts and system/service accounts:**
	1) Identity Creation
	2) Identity provisioning
Unsure if this was addressed appropriately.	3) Attribute maps
	4) Authentication (e.g., password policies and synchronization)

☒ P, Q, N or I Notes: Q – Vendor just listed Y – no description	**6. Security event logging The system must log security information and events.**
	Security Information and Event Management (SIEM) – Splunk
	Cloud Services: Azure, AWS, Oracle, Google
☒ P, Q, N or I	**7. Security Certifications The system must comply too or have the following security certifications:**

Notes:	
Q – need other's input to tell if this meets the requirement.	1) NIST 800-53
	2) FedRamp
	3) HIPAA
	4) SOC 2 Type II
	Note:
	IRS require a 45-day letter approval for new cloud solutions.
☒ P, Q, N or I Notes: Q – Bidder just listed a Y to meet requirement	**8. SIEM (Splunk) integration The system must be able to integrate with the State of Maine Security Information and Event Monitoring (SIEM) Splunk for Security Operations Center operations.**
☒ P, Q, N or I Notes: Q – Bidder just listed a Y to meet requirement	**9. Core constituent data. The system must maintain a central repository of basic (core) constituent data, that can be used by any SoM application to reduce data redundancy and outdated or inaccurate information while maintaining confidentiality.**
☒ P, Q, N or I Notes: Q – Bidder just listed a Y to meet requirement	**11. Data Management. The system must apply the Data Management Rules to the constituent profile data as per the SoM Data Management Policies.**
☒ P, Q, N or I Notes: Q – Bidder just	**12. SOM Employee. The system must support multiple identities for SOM employees that work with the portal in a support role.**

listed a Y to meet requirement	
	1) SOM Employee identity and credentials for supporting the application.
	2) Constituent identity and credentials to use the state services offered through the portal.

☒ P, Q, N or I Notes: Q – Bidder just listed a Y to meet requirement	**13. APIs. The system must be able to connect to at least one agency application.**
	Considerations:
	a) OpenID, OAuth, WS-Fed, SAML, LDAP, Active Directory, Application Programming Interfaces (APIs), Software Development
	b) Develop once and reuse often with other agencies would be ideal
☒ P, Q, N or I Notes: Q – Bidder just listed a Y to meet requirement	**14. User identification matching. The system must be able to match the identity of the portal user to the identity of the same user in the agency system.**
☒ P, Q, N or I Notes: Q – Bidder just listed a Y to meet requirement	**15. Single sign-on. The system must support single sign-on to the agency application.**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Servos
DATE: 5/23/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes: Q – Bidder just listed a Y to meet requirement	**16. Import user profile data from agency systems. The system must be able to import user data from different SoM applications to ensure offboarding happens in a timely manner, so that government resources are protected from fraud. (example: death records)**
☒ P, Q, N or I Notes: Q – Bidder just listed a Y to meet requirement	**17. History logging.** 1) The system must log all actions taken by:
	a) Constituents
	b) MaineIT support
	Including but not limited to:
	c) who made the change
	d) when the change was made
	e) what changed
☒ P, Q, N or I Notes: Q – Bidder just listed a Y to meet requirement	**18. Reporting. The logging data (history) must be available for constituent and system dashboards and reporting in general.**
☒ P, Q, N or I Notes: Q – Bidder just listed a Y to meet requirement and links to documents	**19. Security Controls. The system must comply to the following security controls:**
	1) DDOS Protections[WN1] ,

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Servos
DATE: 5/23/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

	2) OWASP Top 10
	a) Cross Site Scripting,
	b) SQL Injection,
	3) Authentication bypass,
	a) poorly authenticated APIs,
	b) Role based access controls,
	c) proper session control
	4) Real-time visibility,
	5) Anomalous behavior,
	6) User sign with geo-location tracking,
	Geo-blocking capabilities.
	Security controls must include Web Application Firewall [WN1]
☒ P, Q, N or I Notes: Q – Bidder just listed a Y to meet requirement	**20. General System Requirements.** 1) Mobile Support with Native App; (iOS and Android)
	2) System availability: 24/7 with 4x1-hour outages per year
	3) Identity relationships must be tracked in the cloud infrastructure.
	4) Support responsive web and web browsers.
	a. Supports Windows, Chrome, and Macintosh operating systems
☒ P, Q, N or I Notes: Q – Bidder just listed a Y to meet requirement	**21. Training and Support.** 1) Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
	2) MaineIT will require technical/administrator training. There will be initial training and on-going training as users are added.

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Servos
DATE: 5/23/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

	3) Have a continuous process to ensure constituents that may have run into issues setting up accounts can have help 24/7.
☒ P, Q, N or I Notes: Q – Bidder just listed a Y to meet requirement	**22. Support Requirements** 1) The Bidder will provide support, and maintenance for the solution to begin immediately after receiving the State's official acceptance of the implemented solution.
	2) Support and maintenance will be provided for the terms and duration specified in the contract.
	3) The Bidder will address all questions and reported problems related to the technical and functional operation of the system.
	4) The Bidder must provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours: 8:00 a.m. to 5:00 p.m. Eastern Standard Time.
	5) As part of the maintenance agreement, the Bidder will make all product releases and upgrades available to the State at no additional charge.
	6) All release and upgrades shall be implemented and tested by the Bidder, outside of the normal operating hours of the State government.
	7) User testing shall occur during normal State business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State government.
☒ P, Q, N or I Notes: Q – Bidder just listed a Y to meet requirement – I have no idea what their two	**23. Hosting** Solution can comply with MaineIT remote hosting policies. a) Remote Hosting Policy http://maine.gov/oit/policies/RemoteHostingPolicy.pdf b) Hosting Customization Policy http://maine.gov/oit/policies/HostingCustomizationPolicy.pdf

entries represent.	
☒ P, Q, N or I Notes: Q – Bidder just listed a Y to meet requirement, I am unsure if they meet requirements based on their links.	**24. Disaster Recovery** Proposed Solution can comply with MaineIT security requirements and remote hosting requirements, without requiring waivers, before contract finalization.
	1) Maintaining an availability metric of ninety-nine-point nine percent (99.9%) of uptime
	2) Ensuring the capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six hours (i.e., maximum data loss cannot exceed six (6) hours);
	3) Ensuring a recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours;
	4) Ensuring the hosting environment provides adequate capacity to ensure that, under ethernet connectivity to the client device, data inquiry/lookup response is within three (3) seconds, and data modification response is within five (5) seconds;
	5) Providing the Department at least thirty (30) calendar day advance written notice of any material change in network operations or architecture;
	6) Ensuring any planned material change in network operations or architecture cannot be made without the prior written consent of the Department; and Outlining of all Service Level Agreements (SLAs) for technical support (the awarded Bidder shall be open to negotiation to ensure the SLAs meet the Department's needs

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Servos
DATE: 5/23/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

☒1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
P, N, Q, or I & Notes: N – lists SSO as a future goal and does not list 24/7 phone support.

☒1b) Detailed description of the technologies, software and / or hardware for each of the components.
P, N, Q, or I & Notes: N – marketing jargon and bidder states: you might already have an existing ISM system in place.

☒1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.
P, N, Q, or I & Notes: N – lists SSO as a future goal & marketing jargon, very vague

☒1d) Description of the overall platform and architecture of the proposed solution(s).
P, N, Q, or I & Notes: N – marketing jargon

☒1e) Description of any third-party software or partnerships required for the proposed Solution(s).
P, N, Q, or I & Notes: N – vague

☒2a) A detailed timeline and description of milestones, deliverables, tasks
P, N, Q, or I & Notes: N – a graphic, high level, vague

☒2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period
P, N, Q, or I & Notes: I - This plan does not include integrations to different applications

now. We understand that those connections would be scoped during the discovery phase and can impact the overall plan as we could consider a phased approach. This work plan assumes one go live date with core portal and functionality setup.

☒2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
P, N, Q, or I & Notes: P – the work plan only lists three people as part of the project team and DAFS is one of them!

☒2d) Average time to market for each component.
P, N, Q, or I & Notes: P

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. ☒Capture Constituent Identity and profile data.
   P, N, Q, or I & Notes: The link provided for "Preverified flow for Maine" required a login. Q – I only saw one area that addressed data. "The data shared by ID.me to the state agency…" not see anything about capturing profile data but did see a lot about security which this area did not ask for.
b. ☒Provide identity provisioning and deprovisioning.
   P, N, Q, or I & Notes: Q – I am unsure if this meets the requirements.
c. ☒Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
   i. Identity Creation
   ii. Identity provisioning
   iii. Attribute maps
   iv. Authentication (e.g., password policies and synchronization)
      P, N, Q, or I & Notes: Q – I am unsure if this meets the requirements.
d. ☒Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods

currently utilized by State Agencies.
P, N, Q, or I & Notes: P

e. ☒Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
P, N, Q, or I & Notes: Q – I am unsure if this meets the requirements and did not find language around no replication.

f. ☒Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.
P, N, Q, or I & Notes: N – did not see biometrics addresses.

g. ☒Allow for multiple role selections for the following identities:
   i. Individual
   ii. Business Owner
   iii. Support multiple identities for State employees that work with the portal in a support role:
      (a) SOM Employee identity and credentials for supporting the application.
      (b) Constituent identity and credentials to use the state services offered through the portal.
   iv. Multi role individual (Individual and Business Owner)
   P, N, Q, or I & Notes: P

h. ☒Have the ability to provide levels of proofing which will be directly tied to the Constituent's level of consent given.
P, N, Q, or I & Notes: P

i. ☒Support multi-factor authentication to protect against user impersonation and credential theft.
P, N, Q, or I & Notes: P

B.2. ☒The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.
P, N, Q, or I & Notes: P

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Servos
DATE: 5/23/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

a. Disclosure and Consent Management

The desire of the State is to be as transparent as possible and respect the privacy of the individual interacting with the Constituents' Portal. Consent is a core tenant of maintaining the public trust in the Constituents' Portal and will be a foundational component of the architecture.

The Disclosure and Consent Management solution shall include:

i. ☒Granular consent management that encompasses the automated functions necessary to create, modify, revoke, and manage Constituent consents. N – did not address create, modify, revoke – addressed data flowing one way from ID.me to govt.
ii. ☒Allow users the ability to opt-in and opt-out of data sharing and services within the Constituents' portal. P
iii. ☒Obtain user consent both in an interactive and set preference mode for a variety of transactions on the Portal. P
iv. ☒Support administrative users' management of standard legal disclaimers and data classification for transactions. P
v. ☒Highly configurable with version control and history tracking for consent language. N – did not speak to "history tracking." Spoke to privacy.
vi. ☒Ability for end user to access a retrievable log of granted consent and data usage on the portal derived from the consent. P

P, N, Q, or I & Notes: Q – I am unsure if they hit the mark on all of these.

b. Recommendation Technology

The State is seeking options which, while maintaining individual privacy, will collect and analyze data about user interactions, behavior, and preferences. The expected outcome of this will be to provide insights and intelligence that help the State make informed decisions and improve Constituent experiences.

i. ☒From the user perspective, the portal should be able to make real-time recommendations for related services. N "it requires a certain amount of anonymized user data to function effectively." Not promising.
ii. ☒Data captured in this environment must be obfuscated, as to not allow any party to directly target or track the preferences of an individual or their usage of the portal. N - Not promising, said it might limit the effectiveness of engine.

iii. ☒Solution providers should discuss in detail their use, storage, destruction of metadata, and tracking technologies with emphasis on how their offering provides analytical insights while protecting the individual user privacy.

P, N, Q, or I & Notes: N – did not instill promise in 2 of 3 answers.

c. Data Management

The State is seeking the ability for the portal's Constituent identity to be linked to records maintained by individual State agencies. The proposed solution will include:

i. ☒Capabilities to streamline the sharing of data between State systems, including
    i. The identity assurance level
    ii. Agency to user notifications
    iii. Verification of user consent
    iv. Identity resolution
    v. Data sharing between agencies.
ii. ☒Maintain a central repository of basic (core) Constituent data, that can be used by any State application to reduce data redundancy, and outdated or inaccurate information while maintaining confidentiality.
iii. ☒Ability to integrate with State applications using, OpenID, OAuth, Web Services Federation Protocol (WS-Fed), Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), Active Directory, Application Programming Interface (API) or equivalent protocols.
iv. ☒Ability to match the identity of the portal user to the identity of the same user in the Agency system.
v. ☒Log all actions taken by:
    i. Constituents
    ii. MaineIT Support, including:
        (a) Who made the change
        (b) When the change was made
        (c) What changed to and from
vi. ☒Logging data must be available for system dashboards and reporting.

P, N, Q, or I & Notes: I – however they do say that to meet these requirements, might involve additional plugins or customization but does not say if it is included.

d. Customer Service

The State is seeking solution(s) to provide 24/7/365 customer service to Constituents regardless of their location or technical abilities.

  i. ☒Support Constituents with personalized and timely assistance.
  ii. ☒Provide the state options to support our Constituents across multiple channels including, but not limited to phone, email, chat, etc.

P, N, Q, or I & Notes: N – they did provide options, but at an additional cost, it was hard to discern if this covered constituents or the SoM tech people.

C.1. General System

a. ☒Mobile support with native app (iOS and Android)
b. ☒System availability: 24/7 with a maximum of four (4) 1-hour outages per year
c. ☒Identity relationships must be tracked in the cloud infrastructure. N – did not seem to address this, spoke to role, scope based security, not tracking..
d. ☒Support responsive web and web browsers.
  i. ☒Supports Windows, Chrome, and Macintosh operating systems.

P, N, Q, or I & Notes: N – see C.

C.2. ☐Compliance with MaineIT Policies & Standards

a. Architecture Compliance Policy
b. System and Services Acquisition Policy and Procedures (SA-1)
c. Application Deployment Certification Policy
d. Digital Accessibility Policy
e. Remote Hosting Policy
f. Data Exchange Policy
g. Information Security Policy
h. Access Control Policy (AC-1)
i. Access Control Procedures for Users (AC-2)
j. Risk Assessment Policy and Procedures (RA-1)
k. Vulnerability Scanning Procedure (RA-5)
l. Security Assessment and Authorization Policy and Procedures (CA-1)
m. System and Information Integrity Policy and Procedures (SI-1)
n. Configuration Management Policy (CM-1)
o. Web Standards

P, N, Q, or I & Notes: N - As the data controller, the customer is responsible for determining how data is collected, stored, used, shared, archived, destroyed, and maintaining the data's accuracy and confidentiality. Customers are also responsible for meeting the requirements of the relevant privacy legislation in the jurisdictions where they operate and collect personal data. They did not say they would abide by the list of ours.

C.3. Support and Maintenance

a. ☒Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State's official acceptance of the implemented solution.
P, N, Q, or I & Notes:

b. ☒Terms and duration of the support and maintenance will be specified in the contract.
P, N, Q, or I & Notes:

c. ☒All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
P, N, Q, or I & Notes:

d. ☒Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
P, N, Q, or I & Notes:

e. ☒All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
P, N, Q, or I & Notes:

f. ☒All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
P, N, Q, or I & Notes:

g. ☒User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
P, N, Q, or I & Notes: P

4. Security

The proposed solutions must provide a robust security system that aligns with the States Security Policies, standards, and Processes, Including:

Comply with or have the following security certifications:

i. ☐National Institute of Standards and Technology (NIST) 800-53

ii. ☐FedRamp
iii. ☐Health Insurance Portability and Accountability Act (HIPAA)
iv. ☐SOC 2 Type II
v. ☐Comply to the following security controls:
vi. ☐DDOS Protections [WN1]
vii. ☐Open Web Application Security Project (OWASP) Top 10
viii. ☐Cross Site Scripting
ix. ☐Structured Query Language (SQL) Injection
x. ☐Authentication bypass
xi. ☐Poorly authenticated APIs
xii. ☐Role based access controls
xiii. ☐Proper session control
xiv. ☐Real-time visibility
xv. ☐Anomalous behavior
xvi. ☐User sign with geo-location tracking
xvii. ☐Geo-blocking capabilities.
xviii. ☐Web Application Firewall [WN1]
xix. ☐System security must include the following security components:
xx. ☐Account take over protections
xxi. ☐Account sign-in Protections
xxii. ☐Behavior detection and evaluation
xxiii. ☐Adaptive AI Technology
xxiv. ☐Bot Protection; identity visitor behavior through analysis, technical and behavioral data.
xxv. ☐The proposed solution must be able to integrate with the State Security Information and Event Monitoring (SIEM) Splunk. Ability to log security information and events.

P, N, Q, or I & Notes: N – did not specifically address any of these.

5. Licensing

☒The State is aware that multiple licensing options are available and will be required to support the proposed solution in its entirety. The State seeks bids which will provide the most cost-effective licensing approach. Bidders are required to provide a detail breakdown for the proposed licensing.

P, N, Q, or I & Notes: N – contained in cost proposal

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Servos
DATE: 5/23/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

1. Training and OCM (Organizational Change Management)

a. ☐Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
b. ☐Training must include technical and administrator training, initial and ongoing as users are added.
c. ☐Continuous process to ensure Constituents that may have run into issues setting up accounts have help 24/7.
d. ☐Bidders shall guide the State in OCM engagement for the duration of project planning, transition, and final implementation phase including:
  i. Designing and managing team structures with roles and responsibilities to facilitate automated program delivery, while noting any risks anticipated from the lack of readiness in the organization and staffing.
  ii. Ensure a successful transition for the integration of new processes and technology with stakeholders.
  iii. Organizational readiness assessment

P, N, Q, or I & Notes: N – marking jargon and only mentioned train the trainer.

3. Disaster Recovery

a. ☐Availability of ninety-nine-point nine percent (99.9%) of uptime
b. ☐Capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six (6) hours (i.e., maximum data loss cannot exceed six (6) hours)
c. ☐Recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours.

P, N, Q, or I & Notes: N – did not directly address our timelines.

4. Feature Enhancements

a. ☒The State is seeking two hundred and fifty (250) hours of time and material for each proposed technology (CIAM), Personalized Dashboard, Disclosure and Consent Management, Data Management, and Recommendation Technology) to allow for specifications and enhancements during the contract period.

P, N, Q, or I & Notes: N – did not address the 250 hours.

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Servos
DATE: 5/23/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

5. Project Management

a. ☒The State plans to have its own project manager however, the awarded Bidder must have a project manager that has the primary responsibility for executing the project management tasks associated with the project. The awarded Bidder will:
   i. Work in collaboration with the State's Project Manager
   ii. Align with State Project Management processes and practices. – They have their own they state.

b. ☒Manage the implementation, executing all activities, tasks, deliverables and resource needs, both state and awarded Bidder. N – very poorly outlined, does not meet our language.

c. ☒Track project status including managing and tracking all project risks, issues and decisions. N – did not address risks, issues, decisions.

d. ☒Track and report status of deliverables and project status

e. ☒The awarded Bidder will provide their approach for project management and administration services including:
   i. Project Management Methodology
   ii. Project Governance
   iii. Resource Allocation and Schedule Management approach
   iv. Communication Management Approach including status reporting and document repository management.
   v. Risk and Issue Management Methodology
   vi. Change Management Methodology
   vii. Quality Management Methodology

   P, N, Q, or I & Notes: N – did not address hardly any of the requirements to our needs.

D. Value Added Options (Other)

☐Bidders shall provide value added optional services to address relevant matters that have not been anticipated in this RFP but contribute to successful implementation of the proposed solutions, as well as any technology or services that will reduce risk to the project's quality and continuity. The value-added technology and services will not be included in the evaluation process but may be added during the contract negotiations.

P, N, Q, or I & Notes:

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Servos
DATE: 5/23/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Servos
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

Section I – Preliminary Information (No points – Eligibility Requirements)

(File #1 App. A, B, C)
☒Done – Pass/Fail by Procurement & RFP Coordinator

Section II Organization Qualifications and Experience

(File #2 – App. D, E + other areas that have no Appendix number but are part of File #2)

1. **Overview of the Organization (App. D)**
   ☒Bidders must include three examples of projects which demonstrate their experience and expertise in performing these services as well as highlighting the Bidder's stated qualifications and skills.

   Statement of qualifications
   ☒Client name, contact person, Ph#, email.
   Contract history with the state may be considered in rating proposals even if not provided by the bidder.

   P, N, Q, or I & Notes:P

2. **Subcontractors (App. E)**
   ☒If subcontractors are to be used, Bidders must provide the name, address, phone number, contact person, and a brief description of the subcontractors' organizational capacity and qualifications.
   Business name, contact person, address, ph#, email.
   P, N, Q, or I & Notes:P none

3. **Organizational Chart (No Appendix)**
   ☒Bidders must provide an organizational chart. The organizational chart must include the project being proposed. Each position must be identified by position title and corresponding to the personnel job descriptions.
   P, N, Q, or I & Notes: Q not finding

4. **Litigation (No App.)**

☒Bidders must attach a list of all current litigation in which the Bidder is named and a list of all closed cases that have closed within the past five (5) years in which the Bidder paid the claimant either as part of a settlement or by decree. For each, list the entity bringing suit, the complaint, the accusation, amount, and outcome.

P, N, Q, or I & Notes:Q 3 years instead of 5 Years

5. **Financial Viability (No App.)**

☒Bidders must provide a current copy of their Dun & Bradstreet Business Information Report Snapshot.

P, N, Q, or I - Notes: Q not finding

6. **Licensure/Certification (No App.)**

☒Bidders *may* provide documentation of any applicable licensure/certification or specific credentials that are related to providing the proposed services of the RFP.

P, N, Q, or I & Notes:Q not finding

7. **Certificate of Insurance (No App.)**

☐Bidders must provide a certificate of insurance on a standard ACORD form (or the equivalent) evidencing the Bidder's general liability, professional liability and any other relevant liability insurance policies that might be associated with the proposed services.

P, N, Q, or I & Notes:

Section III - Proposed Services

(File #3 – App. F, G, H)

1. **Technical Assessment (App. F)**

☒Done

2. **Services to be Provided (App. G)**

Note: on App. G Detailed Technical and Functional Requirements Excel spreadsheet, a tab is labeled User Stories. No response is required for Tab 3; these were provided to bidders for clarity and understanding of the expected journey a Constituent will experience.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Servos
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes:P	**1. System security components System security must include the following security components:**
	1) Account Take Over Protections
	a) Account Sign-in Protections
	a) Account Sign-in Protections
	a) Adaptive AI Technology
	b) Bot Protection: identify visitor behavior through analysis of technical and behavioral data.
☒ P, Q, N or I Notes: P	**2. Identity Proofing must have the ability to provide levels of proofing which will be directly tied to the constituent's level of access.**
	1) Define various levels of id proofing
	2) Document Image Capture
	3) Close coupling with authentication
☒ P, Q, N or I Notes: P	**3. Multi-factor authentication The system must support multi-factor authentication to protect against user impersonation and credential theft.**
☒ P, Q, N or I Notes: p	**4. Risk-based factors The system must support risk-based factors and scores that are based on factors such as, but not limited to, device and location.**
☒ P, Q, N or I Notes: p	**5. Identity lifecycle management components The system must include the following identity lifecycle management components for risk-based critical applications not limited to end users but also for generic accounts and system/service accounts:**
p	1) Identity Creation
p	2) Identity provisioning
p	3) Attribute maps
p	4) Authentication (e.g., password policies and synchronization)

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Servos
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes:p	**6. Security event logging The system must log security information and events.**
	Security Information and Event Management (SIEM) – Splunk
	Cloud Services: Azure, AWS, Oracle, Google
☒ P, Q, N or I Notes:p	**7. Security Certifications The system must comply too or have the following security certifications:**
p	1) NIST 800-53
p	2) FedRamp
p	3) HIPAA
p	4) SOC 2 Type II
	Note:
	IRS require a 45-day letter approval for new cloud solutions.
☒ P, Q, N or I Notes:p	**8. SIEM (Splunk) integration The system must be able to integrate with the State of Maine Security Information and Event Monitoring (SIEM) Splunk for Security Operations Center operations.**
☒ P, Q, N or I Notes:p	**9. Core constituent data. The system must maintain a central repository of basic (core) constituent data, that can be used by any SoM application to reduce data redundancy and outdated or inaccurate information while maintaining confidentiality.**
☒ P, Q, N or I Notes:p	**11. Data Management. The system must apply the Data Management Rules to the constituent profile data as per the SoM Data Management Policies.**
☒ P, Q, N or I Notes:p	**12. SOM Employee. The system must support multiple identities for SOM employees that work with the portal in a support role.**
p	1) SOM Employee identity and credentials for supporting the application.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Servos
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

p	2) Constituent identity and credentials to use the state services offered through the portal.

☒ P, Q, N or I Notes:p	**13. APIs. The system must be able to connect to at least one agency application.**
	Considerations:
	a) OpenID, OAuth, WS-Fed, SAML, LDAP, Active Directory, Application Programming Interfaces (APIs), Software Development
	b) Develop once and reuse often with other agencies would be ideal
☒ P, Q, N or I Notes:p	**14. User identification matching. The system must be able to match the identity of the portal user to the identity of the same user in the agency system.**
☒ P, Q, N or I Notes:p	**15. Single sign-on. The system must support single sign-on to the agency application.**
☒ P, Q, N or I Notes:p	**16. Import user profile data from agency systems. The system must be able to import user data from different SoM applications to ensure offboarding happens in a timely manner, so that government resources are protected from fraud. (example: death records)**
☒ P, Q, N or I Notes:p	**17. History logging.** 1) The system must log all actions taken by:
p	a) Constituents
p	b) MaineIT support
p	Including but not limited to:
p	c) who made the change
p	d) when the change was made
p	e) what changed

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Servos
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes:p	**18. Reporting. The logging data (history) must be available for constituent and system dashboards and reporting in general.**
☒ P, Q, N or I Notes:p	**19. Security Controls. The system must comply to the following security controls:**
p	1) DDOS Protections[WN1] ,
p	2) OWASP Top 10
p	a) Cross Site Scripting,
p	b) SQL Injection,
p	3) Authentication bypass,
p	a) poorly authenticated APIs,
p	b) Role based access controls,
p	c) proper session control
p	4) Real-time visibility,
p	5) Anomalous behavior,
p	6) User sign with geo-location tracking,
p	Geo-blocking capabilities.
p	Security controls must include Web Application Firewall [WN1]
☒ P, Q, N or I Notes:p	**20. General System Requirements.** 1) Mobile Support with Native App; (iOS and Android)
p	2) System availability: 24/7 with 4x1-hour outages per year
p	3) Identity relationships must be tracked in the cloud infrastructure.
p	4) Support responsive web and web browsers.
p	a. Supports Windows, Chrome, and Macintosh operating systems
☒ P, Q, N or I Notes:p	**21. Training and Support.** 1) Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.

p	2) MaineIT will require technical/administrator training. There will be initial training and on-going training as users are added.
p	3) Have a continuous process to ensure constituents that may have run into issues setting up accounts can have help 24/7.
☒ P, Q, N or I Notes:p	**22. Support Requirements** 1) The Bidder will provide support, and maintenance for the solution to begin immediately after receiving the State's official acceptance of the implemented solution.
p	2) Support and maintenance will be provided for the terms and duration specified in the contract.
p	3) The Bidder will address all questions and reported problems related to the technical and functional operation of the system.
p	4) The Bidder must provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours: 8:00 a.m. to 5:00 p.m. Eastern Standard Time.
p	5) As part of the maintenance agreement, the Bidder will make all product releases and upgrades available to the State at no additional charge.
p	6) All release and upgrades shall be implemented and tested by the Bidder, outside of the normal operating hours of the State government.
p	7) User testing shall occur during normal State business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State government.
☒ P, Q, N or I Notes:p	**23. Hosting** Solution can comply with MaineIT remote hosting policies. a) Remote Hosting Policy http://maine.gov/oit/policies/RemoteHostingPolicy.pdf b) Hosting Customization Policy http://maine.gov/oit/policies/HostingCustomizationPolicy.pdf
☒ P, Q, N or I Notes:p	**24. Disaster Recovery** Proposed Solution can comply with MaineIT security requirements and remote hosting requirements, without requiring waivers, before contract finalization.
p	1) Maintaining an availability metric of ninety-nine-point nine percent (99.9%) of uptime

p	2) Ensuring the capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six hours (i.e., maximum data loss cannot exceed six (6) hours);
p	3) Ensuring a recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours;
p	4) Ensuring the hosting environment provides adequate capacity to ensure that, under ethernet connectivity to the client device, data inquiry/lookup response is within three (3) seconds, and data modification response is within five (5) seconds;
p	5) Providing the Department at least thirty (30) calendar day advance written notice of any material change in network operations or architecture;
p	6) Ensuring any planned material change in network operations or architecture cannot be made without the prior written consent of the Department; and Outlining of all Service Level Agreements (SLAs) for technical support (the awarded Bidder shall be open to negotiation to ensure the SLAs meet the Department's needs

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

☐1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
P, N, Q, or I & Notes: Q high level not detail

☒1b) Detailed description of the technologies, software and / or hardware for each of the components.
P, N, Q, or I & Notes:P

☒1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.
P, N, Q, or I & Notes:P

☒1d) Description of the overall platform and architecture of the proposed solution(s).
P, N, Q, or I & Notes:Q Doesn't say what the presentation layer is

☒1e) Description of any third-party software or partnerships required for the proposed Solution(s).
P, N, Q, or I & Notes:P

☒2a) A detailed timeline and description of milestones, deliverables, tasks
P, N, Q, or I & Notes:P

☒2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period
P, N, Q, or I & Notes:P

☒2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
P, N, Q, or I & Notes:P

☒2d) Average time to market for each component.
P, N, Q, or I & Notes:P

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. ☒Capture Constituent Identity and profile data.
   P, N, Q, or I & Notes:P
b. ☒Provide identity provisioning and deprovisioning.
   P, N, Q, or I & Notes:P

c. ☒Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
   i. Identity Creation
   ii. Identity provisioning
   iii. Attribute maps
   iv. Authentication (e.g., password policies and synchronization)
      P, N, Q, or I & Notes:P

d. ☒Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies.
   P, N, Q, or I & Notes:P

e. ☒Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
   P, N, Q, or I & Notes:P

f. ☒Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.
   P, N, Q, or I & Notes:P

g. ☒Allow for multiple role selections for the following identities:
   i. Individual
   ii. Business Owner
   iii. Support multiple identities for State employees that work with the portal in a support role:
      (a) SOM Employee identity and credentials for supporting the application.
      (b) Constituent identity and credentials to use the state services offered through the portal.
   iv. Multi role individual (Individual and Business Owner)
      P, N, Q, or I & Notes:P

h. ☒Have the ability to provide levels of proofing which will be directly tied to the Constituent's level of consent given.
   P, N, Q, or I & Notes:P

i. ☒Support multi-factor authentication to protect against user impersonation and credential theft.
   P, N, Q, or I & Notes:P

B.2. ☒The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-

stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.
P, N, Q, or I & Notes:P

a. Disclosure and Consent Management

The desire of the State is to be as transparent as possible and respect the privacy of the individual interacting with the Constituents' Portal. Consent is a core tenant of maintaining the public trust in the Constituents' Portal and will be a foundational component of the architecture.

The Disclosure and Consent Management solution shall include:

i. ☒Granular consent management that encompasses the automated functions necessary to create, modify, revoke, and manage Constituent consents.
ii. ☒Allow users the ability to opt-in and opt-out of data sharing and services within the Constituents' portal.
iii. ☒Obtain user consent both in an interactive and set preference mode for a variety of transactions on the Portal.
iv. ☒Support administrative users' management of standard legal disclaimers and data classification for transactions.
v. ☒Highly configurable with version control and history tracking for consent language.
vi. ☒Ability for end user to access a retrievable log of granted consent and data usage on the portal derived from the consent.

P, N, Q, or I & Notes:P

b. Recommendation Technology

The State is seeking options which, while maintaining individual privacy, will collect and analyze data about user interactions, behavior, and preferences. The expected outcome of this will be to provide insights and intelligence that help the State make informed decisions and improve Constituent experiences.

i. ☒From the user perspective, the portal should be able to make real-time recommendations for related services.
ii. ☒Data captured in this environment must be obfuscated, as to not allow any party to directly target or track the preferences of an individual or their usage of the portal.
iii. ☒Solution providers should discuss in detail their use, storage, destruction of metadata, and tracking technologies with emphasis on how their offering provides analytical insights while protecting the individual user privacy.

P, N, Q, or I & Notes:P

c. Data Management

The State is seeking the ability for the portal's Constituent identity to be linked to records maintained by individual State agencies. The proposed solution will include:

i. ☒Capabilities to streamline the sharing of data between State systems, including
    i. The identity assurance level
    ii. Agency to user notifications
    iii. Verification of user consent
    iv. Identity resolution
    v. Data sharing between agencies.
ii. ☒Maintain a central repository of basic (core) Constituent data, that can be used by any State application to reduce data redundancy, and outdated or inaccurate information while maintaining confidentiality.
iii. ☒Ability to integrate with State applications using, OpenID, OAuth, Web Services Federation Protocol (WS-Fed), Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), Active Directory, Application Programming Interface (API) or equivalent protocols.
iv. ☒Ability to match the identity of the portal user to the identity of the same user in the Agency system.
v. ☒Log all actions taken by:
    i. Constituents
    ii. MaineIT Support, including:
        (a) Who made the change
        (b) When the change was made
        (c) What changed to and from
vi. ☒Logging data must be available for system dashboards and reporting.

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Servos
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

P, N, Q, or I & Notes:P

d. Customer Service

The State is seeking solution(s) to provide 24/7/365 customer service to Constituents regardless of their location or technical abilities.

  i. ☒Support Constituents with personalized and timely assistance.
  ii. ☒Provide the state options to support our Constituents across multiple channels including, but not limited to phone, email, chat, etc.

P, N, Q, or I & Notes: Q customer get support through service now portal

C.1. General System

  a. ☒Mobile support with native app (iOS and Android)
  b. ☒System availability: 24/7 with a maximum of four (4) 1-hour outages per year
  c. ☒Identity relationships must be tracked in the cloud infrastructure.
  d. ☒Support responsive web and web browsers.
    i. ☒Supports Windows, Chrome, and Macintosh operating systems.

P, N, Q, or I & Notes:Maintenance of upto 2 hours per month

C.2. ☒Compliance with MaineIT Policies & Standards

  a. Architecture Compliance Policy
  b. System and Services Acquisition Policy and Procedures (SA-1)
  c. Application Deployment Certification Policy
  d. Digital Accessibility Policy
  e. Remote Hosting Policy
  f. Data Exchange Policy
  g. Information Security Policy
  h. Access Control Policy (AC-1)
  i. Access Control Procedures for Users (AC-2)
  j. Risk Assessment Policy and Procedures (RA-1)
  k. Vulnerability Scanning Procedure (RA-5)
  l. Security Assessment and Authorization Policy and Procedures (CA-1)
  m. System and Information Integrity Policy and Procedures (SI-1)
  n. Configuration Management Policy (CM-1)
  o. Web Standards

P, N, Q, or I & Notes:

C.3. Support and Maintenance

a. ☒Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State's official acceptance of the implemented solution.
P, N, Q, or I & Notes:P

b. ☒Terms and duration of the support and maintenance will be specified in the contract.
P, N, Q, or I & Notes:P

c. ☐All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
P, N, Q, or I & Notes:

d. ☐Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
P, N, Q, or I & Notes:

e. ☐All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
P, N, Q, or I & Notes:

f. ☐All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
P, N, Q, or I & Notes:

g. ☐User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
P, N, Q, or I & Notes:Q doesn't specify testing

4. Security

The proposed solutions must provide a robust security system that aligns with the States Security Policies, standards, and Processes, Including:

Comply with or have the following security certifications:

i. ☐National Institute of Standards and Technology (NIST) 800-53

ii. ☐FedRamp
iii. ☐Health Insurance Portability and Accountability Act (HIPAA)
iv. ☐SOC 2 Type II
v. ☐Comply to the following security controls:
vi. ☐DDOS Protections [WN1]
vii. ☐Open Web Application Security Project (OWASP) Top 10
viii. ☐Cross Site Scripting
ix. ☒Structured Query Language (SQL) Injection
x. ☐Authentication bypass
xi. ☐Poorly authenticated APIs
xii. ☐Role based access controls
xiii. ☐Proper session control
xiv. ☐Real-time visibility
xv. ☐Anomalous behavior
xvi. ☐User sign with geo-location tracking
xvii. ☐Geo-blocking capabilities.
xviii. ☐Web Application Firewall [WN1]
xix. ☐System security must include the following security components:
xx. ☐Account take over protections
xxi. ☐Account sign-in Protections
xxii. ☐Behavior detection and evaluation
xxiii. ☐Adaptive AI Technology
xxiv. ☐Bot Protection; identity visitor behavior through analysis, technical and behavioral data.
xxv. ☐The proposed solution must be able to integrate with the State Security Information and Event Monitoring (SIEM) Splunk. Ability to log security information and events.

P, N, Q, or I & Notes:Q service now act as a waf?

5. Licensing

☒The State is aware that multiple licensing options are available and will be required to support the proposed solution in its entirety. The State seeks bids which will provide the most cost-effective licensing approach. Bidders are required to provide a detail breakdown for the proposed licensing.

P, N, Q, or I & Notes:Q don’t have Appendix I

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Servos
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

1. Training and OCM (Organizational Change Management)

a. ☒Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
b. ☒Training must include technical and administrator training, initial and ongoing as users are added.
c. ☒Continuous process to ensure Constituents that may have run into issues setting up accounts have help 24/7.
d. ☒Bidders shall guide the State in OCM engagement for the duration of project planning, transition, and final implementation phase including:
    i. Designing and managing team structures with roles and responsibilities to facilitate automated program delivery, while noting any risks anticipated from the lack of readiness in the organization and staffing.
    ii. Ensure a successful transition for the integration of new processes and technology with stakeholders.
    iii. Organizational readiness assessment

P, N, Q, or I & Notes:Q they offer train the trainer and have training material available.

3. Disaster Recovery

a. ☒Availability of ninety-nine-point nine percent (99.9%) of uptime
b. ☒Capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six (6) hours (i.e., maximum data loss cannot exceed six (6) hours)
c. ☒Recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours.

P, N, Q, or I & Notes:Q Not answered

4. Feature Enhancements

a. ☒The State is seeking two hundred and fifty (250) hours of time and material for each proposed technology (CIAM), Personalized Dashboard, Disclosure and Consent Management, Data Management, and Recommendation Technology) to allow for specifications and enhancements during the contract period.

P, N, Q, or I & Notes:P

5. Project Management

a. ☒The State plans to have its own project manager however, the awarded Bidder must have a project manager that has the primary responsibility for executing the project management tasks associated with the project. The awarded Bidder will:
   i. Work in collaboration with the State's Project Manager
   ii. Align with State Project Management processes and practices.
b. ☒Manage the implementation, executing all activities, tasks, deliverables and resource needs, both state and awarded Bidder.
c. ☒Track project status including managing and tracking all project risks, issues and decisions.
d. ☒Track and report status of deliverables and project status
e. ☒The awarded Bidder will provide their approach for project management and administration services including:
   i. Project Management Methodology
   ii. Project Governance
   iii. Resource Allocation and Schedule Management approach
   iv. Communication Management Approach including status reporting and document repository management.
   v. Risk and Issue Management Methodology
   vi. Change Management Methodology
   vii. Quality Management Methodology

P, N, Q, or I & Notes:P

D. Value Added Options (Other)

☒Bidders shall provide value added optional services to address relevant matters that have not been anticipated in this RFP but contribute to successful implementation of the proposed solutions, as well as any technology or services that will reduce risk to the project's quality and continuity. The value-added technology and services will not be included in the evaluation process but may be added during the contract negotiations.

P, N, Q, or I & Notes:P

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Servos
DATE: 6/12/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Tyler
DATE: 6/10/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

Section I – Preliminary Information (No points – Eligibility Requirements)

(File #1 App. A, B, C)

☒Done – Pass/Fail by Procurement & RFP Coordinator

Section II Organization Qualifications and Experience

(File #2 – App. D, E + other areas that have no Appendix number but are part of File #2)

1. Overview of the Organization (App. D)

☒Bidders must include three examples of projects which demonstrate their experience and expertise in performing these services as well as highlighting the Bidder's stated qualifications and skills.

Statement of qualifications

☒Client name, contact person, Ph#, email.

Contract history with the state may be considered in rating proposals even if not provided by the bidder.

P, N, Q, or **I** & Notes:

Interesting that SoM was a reference

2. Subcontractors (App. E)

☒If subcontractors are to be used, Bidders must provide the name, address, phone number, contact person, and a brief description of the subcontractors' organizational capacity and qualifications.

Business name, contact person, address, ph#, email.

P, N, Q, or **I** & Notes:

3. Organizational Chart (No Appendix)

☒Bidders must provide an organizational chart. The organizational chart must include the project being proposed. Each position must be identified by position title and corresponding to the personnel job descriptions.

P, N, Q, or **I** & Notes:

4. Litigation (No App.)

☒Bidders must attach a list of all current litigation in which the Bidder is named and a list of all closed cases that have closed within the past five (5) years in which the Bidder paid the claimant either as part of a settlement or by decree. For each, list the entity bringing suit, the complaint, the accusation, amount, and outcome.
P, N, Q, or **I** & Notes:

5. Financial Viability (No App.)
☒Bidders must provide a current copy of their Dun & Bradstreet Business Information Report Snapshot.
P, N, Q, or **I** - Notes:

6. Licensure/Certification (No App.)
☒Bidders *may* provide documentation of any applicable licensure/certification or specific credentials that are related to providing the proposed services of the RFP.
P, N, Q, or **I** & Notes:
N/A

7. Certificate of Insurance (No App.)
☒Bidders must provide a certificate of insurance on a standard ACORD form (or the equivalent) evidencing the Bidder's general liability, professional liability and any other relevant liability insurance policies that might be associated with the proposed services.
P, N, Q, or **I** & Notes:

Section III - Proposed Services
(File #3 – App. F, G, H)

1. Technical Assessment (App. F)
☒Done

2. Services to be Provided (App. G)
Note: on App. G Detailed Technical and Functional Requirements Excel spreadsheet, a tab is labeled User Stories. No response is required for Tab 3; these were provided to bidders for clarity and understanding of the expected journey a Constituent will experience.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Tyler
DATE: 6/10/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or **I** Notes:	**1. System security components System security must include the following security components:**
	1) Account Take Over Protections
	a) Account Sign-in Protections
	a) Account Sign-in Protections
	a) Adaptive AI Technology
	b) Bot Protection: identify visitor behavior through analysis of technical and behavioral data.
☒ **P**, Q, N or I Notes:	**2. Identity Proofing must have the ability to provide levels of proofing which will be directly tied to the constituent's level of access.**
	1) Define various levels of id proofing
	2) Document Image Capture
	3) Close coupling with authentication
☒ **P**, Q, N or I Notes:	**3. Multi-factor authentication The system must support multi-factor authentication to protect against user impersonation and credential theft.**
☒ P, Q, N or **I** Notes: location not specifically called out	**4. Risk-based factors The system must support risk-based factors and scores that are based on factors such as, but not limited to, device and location.**
☐ **P**, Q, N or I Notes:	**5. Identity lifecycle management components The system must include the following identity lifecycle management components for risk-based critical applications not limited to end users but also for generic accounts and system/service accounts:**
	1) Identity Creation
Included deprovisioning	2) Identity provisioning
	3) Attribute maps
	4) Authentication (e.g., password policies and synchronization)

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Tyler
DATE: 6/10/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or **I** Notes: Does not mention Socure logging	**6. Security event logging The system must log security information and events.**
	Security Information and Event Management (SIEM) – Splunk
	Cloud Services: Azure, AWS, Oracle, Google
☒ P, Q, N or **I** Notes:	**7. Security Certifications The system must comply too or have the following security certifications:**
	1) NIST 800-53
Solution hosted in fedramp approved cloud; tyler has not deployed	2) FedRamp
	3) HIPAA
No soc 2	4) SOC 2 Type II
	Note:
	IRS require a 45-day letter approval for new cloud solutions.
☒ P, Q, N or **I** Notes: no mention of socure	**8. SIEM (Splunk) integration The system must be able to integrate with the State of Maine Security Information and Event Monitoring (SIEM) Splunk for Security Operations Center operations.**
☒	**9. Core constituent data. The system must maintain a central repository of basic (core) constituent data, that can be used**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Tyler
DATE: 6/10/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

P, Q, **N** or I Notes: does not go into detail on how it reduces or maintains accurate data	**by any SoM application to reduce data redundancy and outdated or inaccurate information while maintaining confidentiality.**
☒ **P**, Q, N or I Notes:	**11. Data Management. The system must apply the Data Management Rules to the constituent profile data as per the SoM Data Management Policies.**
☒ **P**, Q, N or I Notes:	**12. SOM Employee. The system must support multiple identities for SOM employees that work with the portal in a support role.**
	1) SOM Employee identity and credentials for supporting the application.
	2) Constituent identity and credentials to use the state services offered through the portal.

☒ P, Q, N or **I** Notes: LDAP not natively supported; requires Okta addon	**13. APIs. The system must be able to connect to at least one agency application.**
	Considerations:
	a) OpenID, OAuth, WS-Fed, SAML, LDAP, Active Directory, Application Programming Interfaces (APIs), Software Development
	b) Develop once and reuse often with other agencies would be ideal

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Tyler
DATE: 6/10/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

☒ **P**, Q, N or I Notes:	**14. User identification matching. The system must be able to match the identity of the portal user to the identity of the same user in the agency system.**
☒ **P**, Q, N or I Notes:	**15. Single sign-on. The system must support single sign-on to the agency application.**
☒ **P**, Q, N or I Notes:	**16. Import user profile data from agency systems. The system must be able to import user data from different SoM applications to ensure offboarding happens in a timely manner, so that government resources are protected from fraud. (example: death records)**
☒ **P**, Q, N or I Notes:	**17. History logging.** 1) The system must log all actions taken by:
	a) Constituents
	b) MaineIT support
	Including but not limited to:
	c) who made the change
	d) when the change was made
	e) what changed
☒ **P**, Q, N or I Notes:	**18. Reporting. The logging data (history) must be available for constituent and system dashboards and reporting in general.**
☒ P, Q, **N** or I Notes:	**19. Security Controls. The system must comply to the following security controls:**
No detail around how they prevent these controls	1) DDOS Protections[WN1] ,
	2) OWASP Top 10
	a) Cross Site Scripting,
	b) SQL Injection,

	3) Authentication bypass,
	a) poorly authenticated APIs,
	b) Role based access controls,
	c) proper session control
	4) Real-time visibility,
	5) Anomalous behavior,
	6) User sign with geo-location tracking,
	Geo-blocking capabilities.
	Security controls must include Web Application Firewall [WN1]
☒ P, Q, N or **I** Notes:	**20. General System Requirements.** 1) Mobile Support with Native App; (iOS and Android)
Does not call out all products or “the system”	2) System availability: 24/7 with 4x1-hour outages per year
aws	3) Identity relationships must be tracked in the cloud infrastructure.
	4) Support responsive web and web browsers.
	a. Supports Windows, Chrome, and Macintosh operating systems
☒ **P**, Q, N or I Notes:	**21. Training and Support.** 1) Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
	2) MaineIT will require technical/administrator training. There will be initial training and on-going training as users are added.
	3) Have a continuous process to ensure constituents that may have run into issues setting up accounts can have help 24/7.
☒ **P**, Q, N or I Notes:	**22. Support Requirements** 1) The Bidder will provide support, and maintenance for the solution to begin immediately after receiving the State’s official acceptance of the implemented solution.
	2) Support and maintenance will be provided for the terms and duration specified in the contract.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Tyler
DATE: 6/10/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

	3) The Bidder will address all questions and reported problems related to the technical and functional operation of the system.
	4) The Bidder must provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours: 8:00 a.m. to 5:00 p.m. Eastern Standard Time.
	5) As part of the maintenance agreement, the Bidder will make all product releases and upgrades available to the State at no additional charge.
	6) All release and upgrades shall be implemented and tested by the Bidder, outside of the normal operating hours of the State government.
	7) User testing shall occur during normal State business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State government.
☒ **P**, Q, N or I Notes:	**23. Hosting** Solution can comply with MaineIT remote hosting policies. a) Remote Hosting Policy http://maine.gov/oit/policies/RemoteHostingPolicy.pdf b) Hosting Customization Policy http://maine.gov/oit/policies/HostingCustomizationPolicy.pdf
☒ P, Q, N or **I** Notes:	**24. Disaster Recovery** Proposed Solution can comply with MaineIT security requirements and remote hosting requirements, without requiring waivers, before contract finalization.
Again does not call out specific components for uptime just the service in general	1) Maintaining an availability metric of ninety-nine-point nine percent (99.9%) of uptime
	2) Ensuring the capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six hours (i.e., maximum data loss cannot exceed six (6) hours);

	3) Ensuring a recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours;
	4) Ensuring the hosting environment provides adequate capacity to ensure that, under ethernet connectivity to the client device, data inquiry/lookup response is within three (3) seconds, and data modification response is within five (5) seconds;
	5) Providing the Department at least thirty (30) calendar day advance written notice of any material change in network operations or architecture;
	6) Ensuring any planned material change in network operations or architecture cannot be made without the prior written consent of the Department; and Outlining of all Service Level Agreements (SLAs) for technical support (the awarded Bidder shall be open to negotiation to ensure the SLAs meet the Department's needs

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

☒1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
P, N, Q, or I & Notes:
Good break down of how the solution covers the different required areas

☒1b) Detailed description of the technologies, software and / or hardware for each of the components.
P, N, Q, or **I** & Notes:
Okta is rebanded as part of the Tyler native stack; most of lift is Tyler native products

☒1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.
P, N, Q, or I & Notes:
Good detail for how the different requirements (identity, recommendations, consent, etc) interact

☒1d) Description of the overall platform and architecture of the proposed solution(s).

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Tyler
DATE: 6/10/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

P, N, Q, or I & Notes:
detailed mapping logical architecture and flows from both an application and services

☒1e) Description of any third-party software or partnerships required for the proposed Solution(s).
P, **N**, Q, or I & Notes:
While Socure as a software is detailed, no mention of subcontracting work

☒2a) A detailed timeline and description of milestones, deliverables, tasks
P, N, Q, or **I** & Notes:
No called out deliverables

☒2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period
P, **N**, Q, or I & Notes:
No resumes, not all V resources named, no mention of socure C resourcing

☒2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
P, N, Q, or **I** & Notes:
No mention of deliverables

☒2d) Average time to market for each component.
P, N, Q, or **I** & Notes:
Good estimates at time to market values

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. ☒Capture Constituent Identity and profile data.
   P, N, Q, or I & Notes:

Tyler identity is rebranded okta

b. ☒Provide identity provisioning and deprovisioning.
P, N, Q, or I & Notes:
Detailed deprovisioning guides

c. ☒Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
   i. Identity Creation
   ii. Identity provisioning
   iii. Attribute maps
   iv. Authentication (e.g., password policies and synchronization)
      P, N, Q, or I & Notes:

d. ☒Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies.
P, N, Q, or **I** & Notes:
No details around what migration from local to “the solution” of identities look like

e. ☒Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
P, **N,** Q, or I & Notes:
Doesn’t call out explicitly

f. ☒Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.
P, N, Q, or **I** & Notes:
Good call outs for socure and different types of proofing and feature sets available

g. ☒Allow for multiple role selections for the following identities:
   i. Individual
   ii. Business Owner
   iii. Support multiple identities for State employees that work with the portal in a support role:
      (a) SOM Employee identity and credentials for supporting the application.
      (b) Constituent identity and credentials to use the state services offered through the portal.

iv. Multi role individual (Individual and Business Owner)
P, N, Q, or I & Notes:

h. ☐Have the ability to provide levels of proofing which will be directly tied to the Constituent's level of consent given.
P, **N**, Q, or I & Notes:
Missing details around consent

i. ☒Support multi-factor authentication to protect against user impersonation and credential theft.
P, N, Q, or I & Notes:
Via native tyler identity stack

B.2. ☒The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.
P, N, Q, or I & Notes:

a. Disclosure and Consent Management

The desire of the State is to be as transparent as possible and respect the privacy of the individual interacting with the Constituents' Portal. Consent is a core tenant of maintaining the public trust in the Constituents' Portal and will be a foundational component of the architecture.

The Disclosure and Consent Management solution shall include:

i. ☒Granular consent management that encompasses the automated functions necessary to create, modify, revoke, and manage Constituent consents.
ii. ☒Allow users the ability to opt-in and opt-out of data sharing and services within the Constituents' portal.
iii. ☒Obtain user consent both in an interactive and set preference mode for a variety of transactions on the Portal.
iv. ☒Support administrative users' management of standard legal disclaimers and data classification for transactions.

v. ☒Highly configurable with version control and history tracking for consent language.
vi. ☒Ability for end user to access a retrievable log of granted consent and data usage on the portal derived from the consent.

P, N, Q, or I & Notes:

b. Recommendation Technology

The State is seeking options which, while maintaining individual privacy, will collect and analyze data about user interactions, behavior, and preferences. The expected outcome of this will be to provide insights and intelligence that help the State make informed decisions and improve Constituent experiences.

i. ☒From the user perspective, the portal should be able to make real-time recommendations for related services.
ii. ☒Data captured in this environment must be obfuscated, as to not allow any party to directly target or track the preferences of an individual or their usage of the portal.
iii. ☒Solution providers should discuss in detail their use, storage, destruction of metadata, and tracking technologies with emphasis on how their offering provides analytical insights while protecting the individual user privacy.

P, N, Q, or I & Notes:

c. Data Management

The State is seeking the ability for the portal's Constituent identity to be linked to records maintained by individual State agencies. The proposed solution will include:

i. ☒Capabilities to streamline the sharing of data between State systems, including
    i. The identity assurance level
    ii. Agency to user notifications
    iii. Verification of user consent
    iv. Identity resolution
    v. Data sharing between agencies.
ii. ☒Maintain a central repository of basic (core) Constituent data, that can be used by any State application to reduce data redundancy, and outdated or inaccurate information while maintaining confidentiality.
iii. ☒Ability to integrate with State applications using, OpenID, OAuth, Web

Services Federation Protocol (WS-Fed), Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), Active Directory, Application Programming Interface (API) or equivalent protocols.

iv. ☐Ability to match the identity of the portal user to the identity of the same user in the Agency system.

v. ☒Log all actions taken by:
  i. Constituents
  ii. MaineIT Support, including:
    (a) Who made the change
    (b) When the change was made
    (c) What changed to and from

vi. ☒Logging data must be available for system dashboards and reporting.

P, N, Q, or **I** & Notes:

Doesn’t speak to matching identity with agency system/intergration

d. Customer Service

The State is seeking solution(s) to provide 24/7/365 customer service to Constituents regardless of their location or technical abilities.

i. ☒Support Constituents with personalized and timely assistance.

ii. ☒Provide the state options to support our Constituents across multiple channels including, but not limited to phone, email, chat, etc.

P, N, Q, or I & Notes:

C.1. General System

a. ☒Mobile support with native app (iOS and Android)

b. ☒System availability: 24/7 with a maximum of four (4) 1-hour outages per year

c. ☒Identity relationships must be tracked in the cloud infrastructure.

d. ☒Support responsive web and web browsers.
  i. ☒Supports Windows, Chrome, and Macintosh operating systems.

P, N, Q, or I & Notes:

Call outs for all applications and platforms

C.2. ☒Compliance with MaineIT Policies & Standards

a. Architecture Compliance Policy

b. System and Services Acquisition Policy and Procedures (SA-1)

c. Application Deployment Certification Policy

d. Digital Accessibility Policy
e. Remote Hosting Policy
f. Data Exchange Policy
g. Information Security Policy
h. Access Control Policy (AC-1)
i. Access Control Procedures for Users (AC-2)
j. Risk Assessment Policy and Procedures (RA-1)
k. Vulnerability Scanning Procedure (RA-5)
l. Security Assessment and Authorization Policy and Procedures (CA-1)
m. System and Information Integrity Policy and Procedures (SI-1)
n. Configuration Management Policy (CM-1)
o. Web Standards

P, N, Q, or **I** & Notes:

C.3. Support and Maintenance

a. ☐Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State's official acceptance of the implemented solution.
P, **N**, Q, or I & Notes:
Does not specifically call this out

b. ☐Terms and duration of the support and maintenance will be specified in the contract.
P, **N**, Q, or I & Notes:
Does not specifically call this out

c. ☒All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
P, N, Q, or **I** & Notes:

d. ☐Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
P, **N**, Q, or I & Notes: does not call out toll free contact

e. ☒All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
P, N, Q, or **I** & Notes:

f. ☒All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.

P, N, Q, or **I** & Notes:

g. ☒User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
P, N, Q, or **I** & Notes:

4. Security

The proposed solutions must provide a robust security system that aligns with the States Security Policies, standards, and Processes, Including:

Comply with or have the following security certifications:

i. ☒National Institute of Standards and Technology (NIST) 800-53
ii. ☐FedRamp
iii. ☒Health Insurance Portability and Accountability Act (HIPAA)
iv. ☒SOC 2 Type II
v. ☐Comply to the following security controls:
vi. ☐DDOS Protections [WN1]
vii. ☒Open Web Application Security Project (OWASP) Top 10
viii. ☐Cross Site Scripting
ix. ☐Structured Query Language (SQL) Injection
x. ☐Authentication bypass
xi. ☐Poorly authenticated APIs
xii. ☐Role based access controls
xiii. ☐Proper session control
xiv. ☐Real-time visibility
xv. ☐Anomalous behavior
xvi. ☐User sign with geo-location tracking
xvii. ☐Geo-blocking capabilities.
xviii. ☐Web Application Firewall [WN1]
xix. ☐System security must include the following security components:
xx. ☒Account take over protections
xxi. ☒Account sign-in Protections
xxii. ☒Behavior detection and evaluation
xxiii. ☒Adaptive AI Technology
xxiv. ☒Bot Protection; identity visitor behavior through analysis, technical and behavioral data.

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Tyler
DATE: 6/10/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

xxv. ☒The proposed solution must be able to integrate with the State Security Information and Event Monitoring (SIEM) Splunk. Ability to log security information and events.

P, **N**, Q, or **I** & Notes:

Does not specifically call out all requirements, talks to highlevel process and scanning

5. Licensing

☐The State is aware that multiple licensing options are available and will be required to support the proposed solution in its entirety. The State seeks bids which will provide the most cost-effective licensing approach. Bidders are required to provide a detail breakdown for the proposed licensing.

P, **N**, Q, or **I** & Notes:

Not provided

1. Training and OCM (Organizational Change Management)

a. ☒Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
b. ☒Training must include technical and administrator training, initial and ongoing as users are added.
c. ☒Continuous process to ensure Constituents that may have run into issues setting up accounts have help 24/7.
d. ☒Bidders shall guide the State in OCM engagement for the duration of project planning, transition, and final implementation phase including:
    i. Designing and managing team structures with roles and responsibilities to facilitate automated program delivery, while noting any risks anticipated from the lack of readiness in the organization and staffing.
    ii. Ensure a successful transition for the integration of new processes and technology with stakeholders.
    iii. Organizational readiness assessment

P, N, Q, or **I** & Notes:

3. Disaster Recovery

a. ☒Availability of ninety-nine-point nine percent (99.9%) of uptime
b. ☒Capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six (6) hours (i.e., maximum data loss cannot exceed six (6) hours)

c. ☒Recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours.

P, N, Q, or **I** & Notes:
Exceeds requirement

4. Feature Enhancements

a. ☒The State is seeking two hundred and fifty (250) hours of time and material for each proposed technology (CIAM), Personalized Dashboard, Disclosure and Consent Management, Data Management, and Recommendation Technology) to allow for specifications and enhancements during the contract period.

P, N, Q, or **I** & Notes:

5. Project Management

a. ☒The State plans to have its own project manager however, the awarded Bidder must have a project manager that has the primary responsibility for executing the project management tasks associated with the project. The awarded Bidder will:
   i. Work in collaboration with the State’s Project Manager
   ii. Align with State Project Management processes and practices.

b. ☒Manage the implementation, executing all activities, tasks, deliverables and resource needs, both state and awarded Bidder.

c. ☒Track project status including managing and tracking all project risks, issues and decisions.

d. ☒Track and report status of deliverables and project status

e. ☒The awarded Bidder will provide their approach for project management and administration services including:
   i. Project Management Methodology
   ii. Project Governance
   iii. Resource Allocation and Schedule Management approach
   iv. Communication Management Approach including status reporting and document repository management.
   v. Risk and Issue Management Methodology
   vi. Change Management Methodology
   vii. Quality Management Methodology

P, N, Q, or **I** & Notes:

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Tyler
DATE: 6/10/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

D. Value Added Options (Other)

☒Bidders shall provide value added optional services to address relevant matters that have not been anticipated in this RFP but contribute to successful implementation of the proposed solutions, as well as any technology or services that will reduce risk to the project's quality and continuity. The value-added technology and services will not be included in the evaluation process but may be added during the contract negotiations.

P, N, Q, or I & Notes:

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Tyler
DATE: 05 June 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: MaineIT

Section I – Preliminary Information (No points – Eligibility Requirements)

(File #1 App. A, B, C)

☒Done – Pass/Fail by Procurement & RFP Coordinator

Section II Organization Qualifications and Experience

(File #2 – App. D, E + other areas that have no Appendix number but are part of File #2)

1. **Overview of the Organization (App. D)**

   ☒Bidders must include three examples of projects which demonstrate their experience and expertise in performing these services as well as highlighting the Bidder's stated qualifications and skills.
   P: Strong response
   Q: Five examples, instead of three

   Statement of qualifications

   ☒Client name, contact person, Ph#, email.
   Contract history with the state may be considered in rating proposals even if not provided by the bidder.
   P: Strong response
   P: Contract history w/ the state

2. **Subcontractors (App. E)**

   ☒If subcontractors are to be used, Bidders must provide the name, address, phone number, contact person, and a brief description of the subcontractors' organizational capacity and qualifications.
   Business name, contact person, address, ph#, email.
   P: One subcontractor (Socure)

3. **Organizational Chart (No Appendix)**

   ☒Bidders must provide an organizational chart. The organizational chart must include the project being proposed. Each position must be identified by position title and corresponding to the personnel job descriptions.
   P: Adequate response

4. **Litigation (No App.)**

   ☒Bidders must attach a list of all current litigation in which the Bidder is named and a list of all closed cases that have closed within the past five (5) years in which the

Bidder paid the claimant either as part of a settlement or by decree. For each, list the entity bringing suit, the complaint, the accusation, amount, and outcome.

P: Strong response. NO Litigation.

5. **Financial Viability (No App.)**
☒Bidders must provide a current copy of their Dun & Bradstreet Business Information Report Snapshot.
P: Strong response

6. **Licensure/Certification (No App.)**
☒Bidders *may* provide documentation of any applicable licensure/certification or specific credentials that are related to providing the proposed services of the RFP.
N: Weak response

7. **Certificate of Insurance (No App.)**
☒Bidders must provide a certificate of insurance on a standard ACORD form (or the equivalent) evidencing the Bidder's general liability, professional liability and any other relevant liability insurance policies that might be associated with the proposed services.
P: Strong response. $10 MM Cyber Liability.

Section III - Proposed Services

(File #3 – App. F, G, H)

1. **Technical Assessment (App. F)**
☒Done

2. **Services to be Provided (App. G)**

Note: on App. G Detailed Technical and Functional Requirements Excel spreadsheet, a tab is labeled User Stories. No response is required for Tab 3; these were provided to bidders for clarity and understanding of the expected journey a Constituent will experience.

☒ *P: Strong response*	**1. System security components System security must include the following security components:**
	1) Account Take Over Protections
	a) Account Sign-in Protections
	a) Account Sign-in Protections

	a) Adaptive AI Technology
	b) Bot Protection: identify visitor behavior through analysis of technical and behavioral data.
☒ *P: Strong response*	**2. Identity Proofing must have the ability to provide levels of proofing which will be directly tied to the constituent's level of access.**
	1) Define various levels of id proofing
	2) Document Image Capture
	3) Close coupling with authentication
☒ *P: Strong response*	**3. Multi-factor authentication The system must support multi-factor authentication to protect against user impersonation and credential theft.**
☒ *P: Strong response*	**4. Risk-based factors The system must support risk-based factors and scores that are based on factors such as, but not limited to, device and location.**
☒ *P: Strong response*	**5. Identity lifecycle management components The system must include the following identity lifecycle management components for risk-based critical applications not limited to end users but also for generic accounts and system/service accounts:**
	1) Identity Creation
	2) Identity provisioning
	3) Attribute maps
	4) Authentication (e.g., password policies and synchronization)
☒ *N: Weak response. No mention of Socure ID+.*	**6. Security event logging The system must log security information and events.**
	Security Information and Event Management (SIEM) – Splunk
	Cloud Services: Azure, AWS, Oracle, Google

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Tyler
DATE: 05 June 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: MaineIT

☒ *N: Weak response. Does NOT cover Acquia Drupal, Socure ID+.* *N: Did NOT ack the IRS 45-day notice*	**7. Security Certifications The system must comply too or have the following security certifications:**
	1) NIST 800-53
	2) FedRamp
	3) HIPAA
	4) SOC 2 Type II
	Note:
	IRS require a 45-day letter approval for new cloud solutions.
☒ *N: Weak response. No mention of Socure ID+.*	**8. SIEM (Splunk) integration The system must be able to integrate with the State of Maine Security Information and Event Monitoring (SIEM) Splunk for Security Operations Center operations.**
☒ *P: Strong response*	**9. Core constituent data. The system must maintain a central repository of basic (core) constituent data, that can be used by any SoM application to reduce data redundancy and outdated or inaccurate information while maintaining confidentiality.**
☒ *P: Adequate response*	**11. Data Management. The system must apply the Data Management Rules to the constituent profile data as per the SoM Data Management Policies.**
☒ *P: Strong response*	**12. SOM Employee. The system must support multiple identities for SOM employees that work with the portal in a support role.**
	1) SOM Employee identity and credentials for supporting the application.
	2) Constituent identity and credentials to use the state services offered through the portal.
☒	**13. APIs. The system must be able to connect to at least one agency application.**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Tyler
DATE: 05 June 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: MaineIT

P: Strong response	
	Considerations:
	a) OpenID, OAuth, WS-Fed, SAML, LDAP, Active Directory, Application Programming Interfaces (APIs), Software Development
	b) Develop once and reuse often with other agencies would be ideal
☒ *P: Strong response*	**14. User identification matching. The system must be able to match the identity of the portal user to the identity of the same user in the agency system.**
☒ *P: Strong response*	**15. Single sign-on. The system must support single sign-on to the agency application.**
☒ *P: Strong response*	**16. Import user profile data from agency systems. The system must be able to import user data from different SoM applications to ensure offboarding happens in a timely manner, so that government resources are protected from fraud. (example: death records)**
☒ *N: Weak response. No mention of Socure ID+.*	**17. History logging.** 1) The system must log all actions taken by:
	a) Constituents
	b) MaineIT support
	Including but not limited to:
	c) who made the change
	d) when the change was made
	e) what changed
☒ *P: Adequate response*	**18. Reporting. The logging data (history) must be available for constituent and system dashboards and reporting in general.**

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Tyler
DATE: 05 June 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: MaineIT

☒ *N: Weak response. No mention of Socure ID+.*	**19. Security Controls. The system must comply to the following security controls:**
	1) DDOS Protections[WN1] ,
	2) OWASP Top 10
	a) Cross Site Scripting,
	b) SQL Injection,
	3) Authentication bypass,
	a) poorly authenticated APIs,
	b) Role based access controls,
	c) proper session control
	4) Real-time visibility,
	5) Anomalous behavior,
	6) User sign with geo-location tracking,
	Geo-blocking capabilities.
	Security controls must include Web Application Firewall [WN1]
☒ *P: Strong response*	**20. General System Requirements.** 1) Mobile Support with Native App; (iOS and Android)
	2) System availability: 24/7 with 4x1-hour outages per year
	3) Identity relationships must be tracked in the cloud infrastructure.
	4) Support responsive web and web browsers.
	a. Supports Windows, Chrome, and Macintosh operating systems
☒ *P: Adequate response*	**21. Training and Support.** 1) Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
	2) MaineIT will require technical/administrator training. There will be initial training and on-going training as users are added.

	3) Have a continuous process to ensure constituents that may have run into issues setting up accounts can have help 24/7.
☒ *P: Strong response*	**22. Support Requirements** 1) The Bidder will provide support, and maintenance for the solution to begin immediately after receiving the State's official acceptance of the implemented solution.
	2) Support and maintenance will be provided for the terms and duration specified in the contract.
	3) The Bidder will address all questions and reported problems related to the technical and functional operation of the system.
	4) The Bidder must provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours: 8:00 a.m. to 5:00 p.m. Eastern Standard Time.
	5) As part of the maintenance agreement, the Bidder will make all product releases and upgrades available to the State at no additional charge.
	6) All release and upgrades shall be implemented and tested by the Bidder, outside of the normal operating hours of the State government.
	7) User testing shall occur during normal State business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State government.
☒ *N: Weak response. No mention of the other products beyond the native stack: Acquia Drupal, Okta, & Socure ID+.*	**23. Hosting** Solution can comply with MaineIT remote hosting policies. a) Remote Hosting Policy http://maine.gov/oit/policies/RemoteHostingPolicy.pdf b) Hosting Customization Policy http://maine.gov/oit/policies/HostingCustomizationPolicy.pdf
N: Weak response. No mention of the	**24. Disaster Recovery**

other products beyond the native stack: Acquia Drupal, Okta, & Socure ID+.	Proposed Solution can comply with MaineIT security requirements and remote hosting requirements, without requiring waivers, before contract finalization.
	1) Maintaining an availability metric of ninety-nine-point nine percent (99.9%) of uptime
	2) Ensuring the capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six hours (i.e., maximum data loss cannot exceed six (6) hours);
	3) Ensuring a recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours;
	4) Ensuring the hosting environment provides adequate capacity to ensure that, under ethernet connectivity to the client device, data inquiry/lookup response is within three (3) seconds, and data modification response is within five (5) seconds;
	5) Providing the Department at least thirty (30) calendar day advance written notice of any material change in network operations or architecture;
	6) Ensuring any planned material change in network operations or architecture cannot be made without the prior written consent of the Department; and Outlining of all Service Level Agreements (SLAs) for technical support (the awarded Bidder shall be open to negotiation to ensure the SLAs meet the Department's needs

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

☒1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
P: Strong response

☒1b) Detailed description of the technologies, software and / or hardware for each of the components.
P: Strong response

☒1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.
P: Strong response

☒1d) Description of the overall platform and architecture of the proposed solution(s).
P: Strong response

☒1e) Description of any third-party software or partnerships required for the proposed Solution(s).
P: Strong response

☒2a) A detailed timeline and description of milestones, deliverables, tasks
P: Strong response

☒2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period
P: Strong response

☒2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
P: Weak response

☐2d) Average time to market for each component.
N: NO response

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. ☒Capture Constituent Identity and profile data.
   P: Strong response

b. ☒Provide identity provisioning and deprovisioning.
   P: Strong response

c. ☒Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
   i. Identity Creation
   ii. Identity provisioning
   iii. Attribute maps
   iv. Authentication (e.g., password policies and synchronization)
   P: Strong response

d. ☒Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies.
   P: Strong response

e. ☐Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
   N: NO response

f. ☒Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.
   P: Strong response

g. ☒Allow for multiple role selections for the following identities:
   i. Individual
   ii. Business Owner
   iii. Support multiple identities for State employees that work with the portal in a support role:
      (a) SOM Employee identity and credentials for supporting the application.
      (b) Constituent identity and credentials to use the state services offered through the portal.
   iv. Multi role individual (Individual and Business Owner)
   N: Weak response

h. ☐Have the ability to provide levels of proofing which will be directly tied to the Constituent's level of consent given.
   N: NO response

i. ☐Support multi-factor authentication to protect against user impersonation and credential theft.
N: NO response

B.2. ☒The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.
P: Strong response

a. Disclosure and Consent Management
The desire of the State is to be as transparent as possible and respect the privacy of the individual interacting with the Constituents' Portal. Consent is a core tenant of maintaining the public trust in the Constituents' Portal and will be a foundational component of the architecture.
The Disclosure and Consent Management solution shall include:

i. ☒Granular consent management that encompasses the automated functions necessary to create, modify, revoke, and manage Constituent consents.
P: Strong response

ii. ☒Allow users the ability to opt-in and opt-out of data sharing and services within the Constituents' portal.
P: Strong response

iii. ☒Obtain user consent both in an interactive and set preference mode for a variety of transactions on the Portal.
N: Weak response. Only interactive is available, as opposed to set preference mode.

iv. ☒Support administrative users' management of standard legal disclaimers and data classification for transactions.
P: Strong response

v. ☒Highly configurable with version control and history tracking for consent language.
P: Strong response

vi. ☒Ability for end user to access a retrievable log of granted consent and data usage on the portal derived from the consent.
P: Strong response

b. Recommendation Technology

The State is seeking options which, while maintaining individual privacy, will collect and analyze data about user interactions, behavior, and preferences. The expected outcome of this will be to provide insights and intelligence that help the State make informed decisions and improve Constituent experiences.

i. ☒From the user perspective, the portal should be able to make real-time recommendations for related services.
P: Strong response

ii. ☒Data captured in this environment must be obfuscated, as to not allow any party to directly target or track the preferences of an individual or their usage of the portal.
P: Strong response

iii. ☒Solution providers should discuss in detail their use, storage, destruction of metadata, and tracking technologies with emphasis on how their offering provides analytical insights while protecting the individual user privacy.
P: Strong response

c. Data Management

The State is seeking the ability for the portal’s Constituent identity to be linked to records maintained by individual State agencies. The proposed solution will include:

i. ☒Capabilities to streamline the sharing of data between State systems, including
   i. The identity assurance level
   ii. Agency to user notifications
   iii. Verification of user consent
   iv. Identity resolution
   v. Data sharing between agencies.

   P: Strong response

ii. ☒Maintain a central repository of basic (core) Constituent data, that can be used by any State application to reduce data redundancy, and outdated or inaccurate information while maintaining confidentiality.
P: Strong response

iii. ☒Ability to integrate with State applications using, OpenID, OAuth, Web Services Federation Protocol (WS-Fed), Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), Active Directory, Application Programming Interface (API) or equivalent protocols.
P: Strong response

iv. ☒Ability to match the identity of the portal user to the identity of the same user in the Agency system.
P: Strong response

v. ☒Log all actions taken by:
  i. Constituents
  ii. MaineIT Support, including:
    (a) Who made the change
    (b) When the change was made
    (c) What changed to and from
N: Weak response. No mention of Socure ID+.

vi. ☒Logging data must be available for system dashboards and reporting.
N: Weak response. No mention of Socure ID+.

d. Customer Service
The State is seeking solution(s) to provide 24/7/365 customer service to Constituents regardless of their location or technical abilities.
  i. ☒Support Constituents with personalized and timely assistance.
  ii. ☒Provide the state options to support our Constituents across multiple channels including, but not limited to phone, email, chat, etc.
P: Adequate response
N: No mention of other-party products

C.1. General System
  a. ☒Mobile support with native app (iOS and Android)
  b. ☒System availability: 24/7 with a maximum of four (4) 1-hour outages per

year

c. ☒Identity relationships must be tracked in the cloud infrastructure.
d. ☒Support responsive web and web browsers.
  i. ☒Supports Windows, Chrome, and Macintosh operating systems.

P: Adequate response

C.2. ☒Compliance with MaineIT Policies & Standards

a. Architecture Compliance Policy
b. System and Services Acquisition Policy and Procedures (SA-1)
c. Application Deployment Certification Policy
d. Digital Accessibility Policy
e. Remote Hosting Policy
f. Data Exchange Policy
g. Information Security Policy
h. Access Control Policy (AC-1)
i. Access Control Procedures for Users (AC-2)
j. Risk Assessment Policy and Procedures (RA-1)
k. Vulnerability Scanning Procedure (RA-5)
l. Security Assessment and Authorization Policy and Procedures (CA-1)
m. System and Information Integrity Policy and Procedures (SI-1)
n. Configuration Management Policy (CM-1)
o. Web Standards

N: Weak response. No mention of other-party products.

C.3. Support and Maintenance

a. ☒Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State’s official acceptance of the implemented solution.
P: Adequate response

b. ☒Terms and duration of the support and maintenance will be specified in the contract.
P: Adequate response

c. ☒All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
P: Adequate response

d. ☒Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
P: Adequate response

e. ☒All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
P: Adequate response

f. ☒All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
P: Adequate response

g. ☐User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
N: No response

4. Security

The proposed solutions must provide a robust security system that aligns with the States Security Policies, standards, and Processes, Including:

Comply with or have the following security certifications:

i. ☐National Institute of Standards and Technology (NIST) 800-53
ii. ☐FedRamp
iii. ☐Health Insurance Portability and Accountability Act (HIPAA)
iv. ☐SOC 2 Type II
v. ☐Comply to the following security controls:
vi. ☐DDOS Protections [WN1]
vii. ☐Open Web Application Security Project (OWASP) Top 10
viii. ☐Cross Site Scripting
ix. ☐Structured Query Language (SQL) Injection
x. ☐Authentication bypass
xi. ☐Poorly authenticated APIs
xii. ☐Role based access controls
xiii. ☐Proper session control
xiv. ☐Real-time visibility

xv. ☐Anomalous behavior
xvi. ☐User sign with geo-location tracking
xvii. ☐Geo-blocking capabilities.
xviii. ☐Web Application Firewall [WN1]
xix. ☐System security must include the following security components:
xx. ☐Account take over protections
xxi. ☐Account sign-in Protections
xxii. ☐Behavior detection and evaluation
xxiii. ☐Adaptive AI Technology
xxiv. ☐Bot Protection; identity visitor behavior through analysis, technical and behavioral data.
xxv. ☐The proposed solution must be able to integrate with the State Security Information and Event Monitoring (SIEM) Splunk. Ability to log security information and events.

N: Generic response. Does NOT cover the specifics.
N: Weak response. Covers the native stack, Acquia Drupal, & Okta, NOT Socure ID+.

5. Licensing

☒The State is aware that multiple licensing options are available and will be required to support the proposed solution in its entirety. The State seeks bids which will provide the most cost-effective licensing approach. Bidders are required to provide a detail breakdown for the proposed licensing.

P: Adequate response
Q: Synch w/ the Cost Form?

1. Training and OCM (Organizational Change Management)

a. ☐Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
b. ☐Training must include technical and administrator training, initial and ongoing as users are added.
c. ☐Continuous process to ensure Constituents that may have run into issues setting up accounts have help 24/7.
d. ☐Bidders shall guide the State in OCM engagement for the duration of project planning, transition, and final implementation phase including:
    i. Designing and managing team structures with roles and responsibilities to facilitate automated program delivery, while noting any risks anticipated

from the lack of readiness in the organization and staffing.

    ii. Ensure a successful transition for the integration of new processes and technology with stakeholders.
    iii. Organizational readiness assessment

N: Generic boilerplate response. Did NOT address any specifics.

3. **Disaster Recovery**
    a. ☒Availability of ninety-nine-point nine percent (99.9%) of uptime
    b. ☒Capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six (6) hours (i.e., maximum data loss cannot exceed six (6) hours)
    c. ☒Recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours.

P: Strong response

4. **Feature Enhancements**

a. ☒The State is seeking two hundred and fifty (250) hours of time and material for each proposed technology (CIAM), Personalized Dashboard, Disclosure and Consent Management, Data Management, and Recommendation Technology) to allow for specifications and enhancements during the contract period.

P: Adequate response

5. **Project Management**
    a. ☒The State plans to have its own project manager however, the awarded Bidder must have a project manager that has the primary responsibility for executing the project management tasks associated with the project. The awarded Bidder will:
        i. Work in collaboration with the State's Project Manager
        ii. Align with State Project Management processes and practices.
    b. ☒Manage the implementation, executing all activities, tasks, deliverables and resource needs, both state and awarded Bidder.
    c. ☒Track project status including managing and tracking all project risks, issues and decisions.
    d. ☒Track and report status of deliverables and project status
    e. ☒The awarded Bidder will provide their approach for project management and administration services including:
        i. Project Management Methodology
        ii. Project Governance

iii. Resource Allocation and Schedule Management approach
iv. Communication Management Approach including status reporting and document repository management.
v. Risk and Issue Management Methodology
vi. Change Management Methodology
vii. Quality Management Methodology
P: Adequate response

D. Value Added Options (Other)

☒Bidders shall provide value added optional services to address relevant matters that have not been anticipated in this RFP but contribute to successful implementation of the proposed solutions, as well as any technology or services that will reduce risk to the project’s quality and continuity. The value-added technology and services will not be included in the evaluation process but may be added during the contract negotiations.
P: Three concrete options

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Tyler Maine
DATE: 6/4/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

Section I – Preliminary Information (No points – Eligibility Requirements)

(File #1 App. A, B, C)
☒Done – Pass/Fail by Procurement & RFP Coordinator

Section II Organization Qualifications and Experience

(File #2 – App. D, E + other areas that have no Appendix number but are part of File #2)

1. Overview of the Organization (App. D)

☒Bidders must include three examples of projects which demonstrate their experience and expertise in performing these services as well as highlighting the Bidder's stated qualifications and skills.

Statement of qualifications

☒Client name, contact person, Ph#, email.

Contract history with the state may be considered in rating proposals even if not provided by the bidder.

P, N, Q, or I & Notes: P – good examples provided.

2. Subcontractors (App. E)

☒If subcontractors are to be used, Bidders must provide the name, address, phone number, contact person, and a brief description of the subcontractors' organizational capacity and qualifications.
Business name, contact person, address, ph#, email.
P, N, Q, or I & Notes: P

3. Organizational Chart (No Appendix)

☒Bidders must provide an organizational chart. The organizational chart must include the project being proposed. Each position must be identified by position title and corresponding to the personnel job descriptions.
P, N, Q, or I & Notes: P

4. Litigation (No App.)

☒Bidders must attach a list of all current litigation in which the Bidder is named and a list of all closed cases that have closed within the past five (5) years in which the Bidder paid the claimant either as part of a settlement or by decree. For each, list the entity bringing suit, the complaint, the accusation, amount, and outcome.
P, N, Q, or I & Notes: P

5. **Financial Viability (No App.)**
☒Bidders must provide a current copy of their Dun & Bradstreet Business Information Report Snapshot.
P, N, Q, or I - Notes: P – extensive information shared.

6. **Licensure/Certification (No App.)**
☒Bidders *may* provide documentation of any applicable licensure/certification or specific credentials that are related to providing the proposed services of the RFP.
P, N, Q, or I & Notes: P

7. **Certificate of Insurance (No App.)**
☒Bidders must provide a certificate of insurance on a standard ACORD form (or the equivalent) evidencing the Bidder's general liability, professional liability and any other relevant liability insurance policies that might be associated with the proposed services.
P, N, Q, or I & Notes: P

Section III - Proposed Services

(File #3 – App. F, G, H)

1. **Technical Assessment (App. F)**
☒Done

2. **Services to be Provided (App. G)**

Note: on App. G Detailed Technical and Functional Requirements Excel spreadsheet, a tab is labeled User Stories. No response is required for Tab 3; these were provided to bidders for clarity and understanding of the expected journey a Constituent will experience.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Tyler Maine
DATE: 6/4/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes: P	**1. System security components System security must include the following security components:**
	1) Account Take Over Protections
	a) Account Sign-in Protections
	a) Account Sign-in Protections
	a) Adaptive AI Technology
	b) Bot Protection: identify visitor behavior through analysis of technical and behavioral data.
☒ P, Q, N or I Notes: P	**2. Identity Proofing must have the ability to provide levels of proofing which will be directly tied to the constituent's level of access.**
	1) Define various levels of id proofing
	2) Document Image Capture
	3) Close coupling with authentication
☒ P, Q, N or I Notes: P	**3. Multi-factor authentication The system must support multi-factor authentication to protect against user impersonation and credential theft.**
☒ P, Q, N or I Notes: P	**4. Risk-based factors The system must support risk-based factors and scores that are based on factors such as, but not limited to, device and location.**
☒ P, Q, N or I Notes: P	**5. Identity lifecycle management components The system must include the following identity lifecycle management components for risk-based critical applications not limited to end users but also for generic accounts and system/service accounts:**
	1) Identity Creation
	2) Identity provisioning – nice description of the two ways to deactivate accounts
	3) Attribute maps
	4) Authentication (e.g., password policies and synchronization)

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Tyler Maine
DATE: 6/4/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes: P	**6. Security event logging The system must log security information and events.**
	Security Information and Event Management (SIEM) – Splunk
	Cloud Services: Azure, AWS, Oracle, Google
☒ P, Q, N or I Notes: P	**7. Security Certifications The system must comply too or have the following security certifications:**
	1) NIST 800-53
	2) FedRamp
	3) HIPAA
	4) SOC 2 Type II
	Note:
	IRS require a 45-day letter approval for new cloud solutions.
☒ P, Q, N or I Notes: P	**8. SIEM (Splunk) integration The system must be able to integrate with the State of Maine Security Information and Event Monitoring (SIEM) Splunk for Security Operations Center operations.**
☒ P, Q, N or I Notes: P	**9. Core constituent data. The system must maintain a central repository of basic (core) constituent data, that can be used by any SoM application to reduce data redundancy and outdated or inaccurate information while maintaining confidentiality.**
☒ P, Q, N or I Notes: P	**11. Data Management. The system must apply the Data Management Rules to the constituent profile data as per the SoM Data Management Policies.**
☒ P, Q, N or I Notes: P	**12. SOM Employee. The system must support multiple identities for SOM employees that work with the portal in a support role.**
	1) SOM Employee identity and credentials for supporting the application.

	2) Constituent identity and credentials to use the state services offered through the portal.

☒ P, Q, N or I Notes: P	**13. APIs. The system must be able to connect to at least one agency application.**
	Considerations:
	a) OpenID, OAuth, WS-Fed, SAML, LDAP, Active Directory, Application Programming Interfaces (APIs), Software Development
	b) Develop once and reuse often with other agencies would be ideal
☒ P, Q, N or I Notes: P	**14. User identification matching. The system must be able to match the identity of the portal user to the identity of the same user in the agency system.**
☐ P, Q, N or I Notes:	**15. Single sign-on. The system must support single sign-on to the agency application.**
☒ P, Q, N or I Notes: P	**16. Import user profile data from agency systems. The system must be able to import user data from different SoM applications to ensure offboarding happens in a timely manner, so that government resources are protected from fraud. (example: death records)**
☒ P, Q, N or I Notes: P	**17. History logging.** 1) The system must log all actions taken by:
	a) Constituents
	b) MaineIT support
	Including but not limited to:
	c) who made the change
	d) when the change was made
	e) what changed

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Tyler Maine
DATE: 6/4/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes: P	**18. Reporting. The logging data (history) must be available for constituent and system dashboards and reporting in general.**
☒ P, Q, N or I Notes: P	**19. Security Controls. The system must comply to the following security controls:**
	1) DDOS Protections[WN1] ,
	2) OWASP Top 10
	a) Cross Site Scripting,
	b) SQL Injection,
	3) Authentication bypass,
	a) poorly authenticated APIs,
	b) Role based access controls,
	c) proper session control
	4) Real-time visibility,
	5) Anomalous behavior,
	6) User sign with geo-location tracking,
	Geo-blocking capabilities.
	Security controls must include Web Application Firewall [WN1]
☒ P, Q, N or I Notes: P	**20. General System Requirements.** 1) Mobile Support with Native App; (iOS and Android)
	2) System availability: 24/7 with 4x1-hour outages per year
	3) Identity relationships must be tracked in the cloud infrastructure.
	4) Support responsive web and web browsers.
	a. Supports Windows, Chrome, and Macintosh operating systems
☒ P, Q, N or I Notes: P	**21. Training and Support.** 1) Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.

	2) MaineIT will require technical/administrator training. There will be initial training and on-going training as users are added.
	3) Have a continuous process to ensure constituents that may have run into issues setting up accounts can have help 24/7.
☒ P, Q, N or I Notes: P	**22. Support Requirements** 1) The Bidder will provide support, and maintenance for the solution to begin immediately after receiving the State's official acceptance of the implemented solution.
	2) Support and maintenance will be provided for the terms and duration specified in the contract.
	3) The Bidder will address all questions and reported problems related to the technical and functional operation of the system.
	4) The Bidder must provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours: 8:00 a.m. to 5:00 p.m. Eastern Standard Time.
	5) As part of the maintenance agreement, the Bidder will make all product releases and upgrades available to the State at no additional charge.
	6) All release and upgrades shall be implemented and tested by the Bidder, outside of the normal operating hours of the State government.
	7) User testing shall occur during normal State business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State government.
☒ P, Q, N or I Notes: P	**23. Hosting** Solution can comply with MaineIT remote hosting policies. a) Remote Hosting Policy http://maine.gov/oit/policies/RemoteHostingPolicy.pdf b) Hosting Customization Policy http://maine.gov/oit/policies/HostingCustomizationPolicy.pdf
☒ P, Q, N or I Notes: P	**24. Disaster Recovery** Proposed Solution can comply with MaineIT security requirements and remote hosting requirements, without requiring waivers, before contract finalization.
	1) Maintaining an availability metric of ninety-nine-point nine percent (99.9%) of uptime

	2) Ensuring the capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six hours (i.e., maximum data loss cannot exceed six (6) hours);
	3) Ensuring a recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours;
	4) Ensuring the hosting environment provides adequate capacity to ensure that, under ethernet connectivity to the client device, data inquiry/lookup response is within three (3) seconds, and data modification response is within five (5) seconds;
	5) Providing the Department at least thirty (30) calendar day advance written notice of any material change in network operations or architecture;
	6) Ensuring any planned material change in network operations or architecture cannot be made without the prior written consent of the Department; and Outlining of all Service Level Agreements (SLAs) for technical support (the awarded Bidder shall be open to negotiation to ensure the SLAs meet the Department's needs

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

☒1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
P, N, Q, or I & Notes: P – good inclusion of legacy services. Great description of the Resident Engagement Platform and Mycivic. Pg. 7, people and information piece, maps, local historic sites, surveys, feedback forms all detailed. Engagement Builder looks like a powerful tool for admins and agency users to use. Data insights through their tool, used to be Socrata, very well done.Pg 12

☒1b) Detailed description of the technologies, software and / or hardware for each of the components.
P, N, Q, or I & Notes: P

☐1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.

P, N, Q, or I & Notes: P

☐1d) Description of the overall platform and architecture of the proposed solution(s).
P, N, Q, or I & Notes: P

☐1e) Description of any third-party software or partnerships required for the proposed Solution(s).
P, N, Q, or I & Notes: P – well done!

☒2a) A detailed timeline and description of milestones, deliverables, tasks
P, N, Q, or I & Notes: P

☒2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through Implementation Period and Post Implementation – Support period
P, N, Q, or I & Notes: P

☒2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
P, N, Q, or I & Notes: P

☒2d) Average time to market for each component.
P, N, Q, or I & Notes: P

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. ☒Capture Constituent Identity and profile data.

P, N, Q, or I & Notes: P

b. ☒Provide identity provisioning and deprovisioning.
P, N, Q, or I & Notes: P pg. 24

c. ☒Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
   i. Identity Creation
   ii. Identity provisioning
   iii. Attribute maps

Authentication (e.g., password policies and synchronization)
P, N, Q, or I & Notes: P – very thorough descriptions. !

Data-Driven Deactivation: The system can automatically deactivate accounts based on government data, such as death records, indicating account inactivity or when the system detects fraud.

   iv.

d. ☒Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies.
P, N, Q, or I & Notes: P

☒Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
P, N, Q, or I & Notes: P - As a longstanding technology partner of the State of Maine, Tyler possesses an in-depth understanding of your existing service portfolio. We are committed to collaborating closely with each stakeholder agency to seamlessly integrate the value proposition of the Constituent Portal with their existing services, while ensuring the continued effectiveness of standalone service channels. This collaborative approach ensures a smooth transition and maximizes the benefits of the platform for both constituents and State agencies.

e.

f. ☒Describe the extensibility of architecture so that future means of identity-proofing (e.g. biometrics) may be incorporated.
P, N, Q, or I & Notes: P- very thorough answer. SocureID+ goes all the way in for identity proofing, risk score criteria!. Pg 27. Redundant data sources, pg. 30. Meetins NIST Liveness Presentation Attack Detention Level 2. Biometric match & high accuracy if individual is present when transaction is taking place.

g. ☒Allow for multiple role selections for the following identities:
   i. Individual
   ii. Business Owner – Tyler adds in a Business profile separate identity and can assign roles within this profile , once created a business can invite others CIAM users to participate in the business profile!

iii. Support multiple identities for State employees that work with the portal in a support role:
    (a) SOM Employee identity and credentials for supporting the application. New employees are granted immediate access to administrative tools upon hire, automatically terminated on departure. Managed via Maine's security policies.
    (b) Constituent identity and credentials to use the state services offered through the portal.
iv. Multi role individual (Individual and Business Owner)
    P, N, Q, or I & Notes: P

h. ☒Have the ability to provide levels of proofing which will be directly tied to the Constituent's level of consent given.
   P, N, Q, or I & Notes: P

i. ☒Support multi-factor authentication to protect against user impersonation and credential theft.
   P, N, Q, or I & Notes: P

B.2. ☒The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.
P, N, Q, or I & Notes: P – events calendar, dedicated inbox, organized – categorized repository of all documents related to resident. Resume unfinished business -saved sessions, history of all engagements the user had made with the portal. Feedback channel. GREAT mock up of site: pg. 35. Calendars can include renewals as well as fairs, holidays. You can set trigger events. Upon completion of a digital service, a future event can automatically created to remind user to revisit and repeat the transaction. Secure document vault! Transaction receipts, permits licences, official documents.Public safety alerts, location specific alerts, The Resident Engagement Platform is full of top notch qualities.

a. Disclosure and Consent Management

The desire of the State is to be as transparent as possible and respect the privacy of the individual interacting with the Constituents' Portal. Consent is a core tenant of maintaining the public trust in the Constituents' Portal and will be a foundational component of the architecture.

The Disclosure and Consent Management solution shall include:

i. ☒Granular consent management that encompasses the automated functions necessary to create, modify, revoke, and manage Constituent consents.
ii. ☒Allow users the ability to opt-in and opt-out of data sharing and services within the Constituents' portal.
iii. ☒Obtain user consent both in an interactive and set preference mode for a variety of transactions on the Portal.
iv. ☒Support administrative users' management of standard legal disclaimers and data classification for transactions.
v. ☒Highly configurable with version control and history tracking for consent language.
vi. ☒Ability for end user to access a retrievable log of granted consent and data usage on the portal derived from the consent.

P, N, Q, or I & Notes: P – Cookie consent module even! Pg. 40 – list of many consents user can control. Second party data sharing. Pg. 41, pg. 43 – when consent language is changed down the road, users are alerted to the change so they can consent again if they agree.

b. Recommendation Technology

The State is seeking options which, while maintaining individual privacy, will collect and analyze data about user interactions, behavior, and preferences. The expected outcome of this will be to provide insights and intelligence that help the State make informed decisions and improve Constituent experiences.

i. ☒From the user perspective, the portal should be able to make real-time recommendations for related services. Machine learning recommendations feature is great. Anonymization strategy for using synthetic identifiers.
ii. ☒Data captured in this environment must be obfuscated, as to not allow any party to directly target or track the preferences of an individual or their usage of the portal.

iii. ☒Solution providers should discuss in detail their use, storage, destruction of metadata, and tracking technologies with emphasis on how their offering provides analytical insights while protecting the individual user privacy.

P, N, Q, or I & Notes: P - Engagement dashboard – decision makers can measure the success and reach of the program, seeing current info about constituent use.
Pg. 48

c. Data Management
The State is seeking the ability for the portal's Constituent identity to be linked to records maintained by individual State agencies. The proposed solution will include:

i. ☒Capabilities to streamline the sharing of data between State systems, including
    i. The identity assurance level
    ii. Agency to user notifications – to a dedicated inbox on their portal.
    iii. Verification of user consent
    iv. Identity resolution
    v. Data sharing between agencies.
ii. ☒Maintain a central repository of basic (core) Constituent data, that can be used by any State application to reduce data redundancy, and outdated or inaccurate information while maintaining confidentiality.
iii. ☒Ability to integrate with State applications using, OpenID, OAuth, Web Services Federation Protocol (WS-Fed), Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), Active Directory, Application Programming Interface (API) or equivalent protocols.
iv. ☒Ability to match the identity of the portal user to the identity of the same user in the Agency system.
v. ☒Log all actions taken by:
    i. Constituents
    ii. MaineIT Support, including:
        (a) Who made the change
        (b) When the change was made
        (c) What changed to and from
vi. ☒Logging data must be available for system dashboards and reporting.

P, N, Q, or I & Notes: P – All activity taken by constituents is logged in the engagement platform

d. Customer Service
The State is seeking solution(s) to provide 24/7/365 customer service to Constituents regardless of their location or technical abilities.
  i. ☒Support Constituents with personalized and timely assistance.
  ii. ☒Provide the state options to support our Constituents across multiple channels including, but not limited to phone, email, chat, etc.

P, N, Q, or I & Notes: P

C.1. General System
- a. ☒Mobile support with native app (iOS and Android)
- b. ☒System availability: 24/7 with a maximum of four (4) 1-hour outages per year
- c. ☒Identity relationships must be tracked in the cloud infrastructure.
- d. ☒Support responsive web and web browsers.
  - i. ☒Supports Windows, Chrome, and Macintosh operating systems.

P, N, Q, or I & Notes: P

C.2. ☐Compliance with MaineIT Policies & Standards
- a. Architecture Compliance Policy
- b. System and Services Acquisition Policy and Procedures (SA-1)
- c. Application Deployment Certification Policy
- d. Digital Accessibility Policy
- e. Remote Hosting Policy
- f. Data Exchange Policy
- g. Information Security Policy
- h. Access Control Policy (AC-1)
- i. Access Control Procedures for Users (AC-2)
- j. Risk Assessment Policy and Procedures (RA-1)
- k. Vulnerability Scanning Procedure (RA-5)
- l. Security Assessment and Authorization Policy and Procedures (CA-1)
- m. System and Information Integrity Policy and Procedures (SI-1)
- n. Configuration Management Policy (CM-1)
- o. Web Standards

P, N, Q, or I & Notes: P -= In crafting our solution and proposal, our team conducted a comprehensive review of each MaineIT policy and standard identified within the RFP. Following this in-depth analysis and internal discussions, we confidently conclude that our proposed solution aligns fully with all applicable policies and standards, and do not anticipate needing to request exemptions from these policies and standards We will collaborate with the State to fully understand the impact of changes in policies and standards, and work to ensure the Constituent Portal maintains its compliance posture throughout the term of the contract

C.3. Support and Maintenance

a. ☒Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State's official acceptance of the implemented solution.
P, N, Q, or I & Notes:

b. ☒Terms and duration of the support and maintenance will be specified in the contract.
P, N, Q, or I & Notes:

c. ☒All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
P, N, Q, or I & Notes:

d. ☒Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
P, N, Q, or I & Notes:

e. ☒All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
P, N, Q, or I & Notes:

f. ☒All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
P, N, Q, or I & Notes:

g. ☒User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
P, N, Q, or I & Notes:
P on all sections above.

4. Security

The proposed solutions must provide a robust security system that aligns with the States Security Policies, standards, and Processes, Including:

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Tyler Maine
DATE: 6/4/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

Comply with or have the following security certifications:

i. ☐National Institute of Standards and Technology (NIST) 800-53
ii. ☐FedRamp
iii. ☐Health Insurance Portability and Accountability Act (HIPAA)
iv. ☐SOC 2 Type II
v. ☐Comply to the following security controls:
vi. ☐DDOS Protections [WN1]
vii. ☐Open Web Application Security Project (OWASP) Top 10
viii. ☐Cross Site Scripting
ix. ☐Structured Query Language (SQL) Injection
x. ☐Authentication bypass
xi. ☐Poorly authenticated APIs
xii. ☐Role based access controls
xiii. ☐Proper session control
xiv. ☐Real-time visibility
xv. ☐Anomalous behavior
xvi. ☐User sign with geo-location tracking
xvii. ☐Geo-blocking capabilities.
xviii. ☐Web Application Firewall [WN1]
xix. ☐System security must include the following security components:
xx. ☐Account take over protections
xxi. ☐Account sign-in Protections
xxii. ☐Behavior detection and evaluation
xxiii. ☐Adaptive AI Technology
xxiv. ☐Bot Protection; identity visitor behavior through analysis, technical and behavioral data.
xxv. ☐The proposed solution must be able to integrate with the State Security Information and Event Monitoring (SIEM) Splunk. Ability to log security information and events.

P, N, Q, or I & Notes: P – Tyler will establish a Security Management Vulnerability Program to account for the overall security of the proposed Maine Constituent Portal. This will ensure regular security evaluations and analysis, while providing the State with transparency into the current state of security related items through regular communications and reports. Answered all above very well.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Tyler Maine
DATE: 6/4/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

5. Licensing

☒The State is aware that multiple licensing options are available and will be required to support the proposed solution in its entirety. The State seeks bids which will provide the most cost-effective licensing approach. Bidders are required to provide a detail breakdown for the proposed licensing.

P, N, Q, or I & Notes: P – Tyler provides the licensing to the 3rd party providers proposed in their solution.

1. Training and OCM (Organizational Change Management)

a. ☒Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
b. ☒Training must include technical and administrator training, initial and ongoing as users are added.
c. ☒Continuous process to ensure Constituents that may have run into issues setting up accounts have help 24/7.
d. ☒Bidders shall guide the State in OCM engagement for the duration of project planning, transition, and final implementation phase including:
   i. Designing and managing team structures with roles and responsibilities to facilitate automated program delivery, while noting any risks anticipated from the lack of readiness in the organization and staffing.
   ii. Ensure a successful transition for the integration of new processes and technology with stakeholders.
   iii. Organizational readiness assessment

P, N, Q, or I & Notes: P – Tyler will onboard a training resource for the portal. Following the development of each Portal component, the training resource will partner with the Tyler and State Project Managers to author a training plan that aligns with Maine's unique implementation. This will ensure that a comprehensive training plan is drafted alongside the completed solution. Pg. 68. Tyler will work with the Constituent Portal Project Manager and other State leaders to identify a core group of IT and agency staff willing and interested in understanding the solution at a deeper level than the standard training offering would provide. the Tyler Project Manager will partner closely with the State Project Manager to identify the State resources and processes that will be required to onboard a new agency into the Constituent Portal, such as MaineIT staff and Deployment Certification process. Once identified, a step-by-step onboarding guide will be created and workshopped using a sample agency. Gaps and challenges identified through the sample agency exercise will drive the development of an Organizational Readiness Assessment form, which will eventually serve as the first step for agencies interested in integrating the Constituent Portal in their services.

3. **Disaster Recovery**
    a. ☒Availability of ninety-nine-point nine percent (99.9%) of uptime
    b. ☒Capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six (6) hours (i.e., maximum data loss cannot exceed six (6) hours)
    c. ☐Recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours.

P, N, Q, or I & Notes: P

4. **Feature Enhancements**

a. ☒The State is seeking two hundred and fifty (250) hours of time and material for each proposed technology (CIAM), Personalized Dashboard, Disclosure and Consent Management, Data Management, and Recommendation Technology) to allow for specifications and enhancements during the contract period.

P, N, Q, or I & Notes: P

5. **Project Management**
    a. ☒The State plans to have its own project manager however, the awarded Bidder must have a project manager that has the primary responsibility for executing the project management tasks associated with the project. The awarded Bidder will:
        i. Work in collaboration with the State's Project Manager – allow editing privileges to their Gantt chart if desired.
        ii. Align with State Project Management processes and practices.
    b. ☐Manage the implementation, executing all activities, tasks, deliverables and resource needs, both state and awarded Bidder.
    c. ☒Track project status including managing and tracking all project risks, issues and decisions.
    d. ☒Track and report status of deliverables and project status
    e. ☒The awarded Bidder will provide their approach for project management and administration services including:

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Tyler Maine
DATE: 6/4/24
EVALUATOR NAME: Lisa Leahy
EVALUATOR DEPARTMENT: MaineIT

i. Project Management Methodology
ii. Project Governance
iii. Resource Allocation and Schedule Management approach
iv. Communication Management Approach including status reporting and document repository management.
v. Risk and Issue Management Methodology
vi. Change Management Methodology
vii. Quality Management Methodology

P, N, Q, or I & Notes: P -
Implement internal and external communication plan. A tiered governance approach is suggested and it's very thorough.

D. Value Added Options (Other)

☒Bidders shall provide value added optional services to address relevant matters that have not been anticipated in this RFP but contribute to successful implementation of the proposed solutions, as well as any technology or services that will reduce risk to the project's quality and continuity. The value-added technology and services will not be included in the evaluation process but may be added during the contract negotiations.

P, N, Q, or I & Notes: p – digital wallet Pg 76., batch scrub for legacy apps.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Tyler
DATE: 6/11/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

Section I – Preliminary Information (No points – Eligibility Requirements)

(File #1 App. A, B, C)

☒Done – Pass/Fail by Procurement & RFP Coordinator

Section II Organization Qualifications and Experience

(File #2 – App. D, E + other areas that have no Appendix number but are part of File #2)

1. Overview of the Organization (App. D)

☒Bidders must include three examples of projects which demonstrate their experience and expertise in performing these services as well as highlighting the Bidder's stated qualifications and skills.

Statement of qualifications

☒Client name, contact person, Ph#, email.

Contract history with the state may be considered in rating proposals even if not provided by the bidder.

P, N, Q, or I & Notes:P, Provided five examples

2. Subcontractors (App. E)

☒If subcontractors are to be used, Bidders must provide the name, address, phone number, contact person, and a brief description of the subcontractors' organizational capacity and qualifications.

Business name, contact person, address, ph#, email.

P, N, Q, or I & Notes:Q, listed 1 subcontractor Missing 2 other product Okta and Drupal

3. Organizational Chart (No Appendix)

☒Bidders must provide an organizational chart. The organizational chart must include the project being proposed. Each position must be identified by position title and corresponding to the personnel job descriptions.

P, N, Q, or I & Notes:P. Chart provded

4. Litigation (No App.)

☒Bidders must attach a list of all current litigation in which the Bidder is named and a list of all closed cases that have closed within the past five (5) years in which the Bidder paid the claimant either as part of a settlement or by decree. For each, list the entity bringing suit, the complaint, the accusation, amount, and outcome.
P, N, Q, or I & Notes:P. No ligations

5. **Financial Viability (No App.)**
☒Bidders must provide a current copy of their Dun & Bradstreet Business Information Report Snapshot.
P, N, Q, or I - Notes:P. Provided and is in good standing

6. **Licensure/Certification (No App.)**
☐Bidders *may* provide documentation of any applicable licensure/certification or specific credentials that are related to providing the proposed services of the RFP.
P, N, Q, or I & Notes:Says not required

7. **Certificate of Insurance (No App.)**
☒Bidders must provide a certificate of insurance on a standard ACORD form (or the equivalent) evidencing the Bidder's general liability, professional liability and any other relevant liability insurance policies that might be associated with the proposed services.
P, N, Q, or I & Notes:P. Provided liability insurance.

Section III - Proposed Services
(File #3 – App. F, G, H)

1. **Technical Assessment (App. F)**
☒Done

2. **Services to be Provided (App. G)**

Note: on App. G Detailed Technical and Functional Requirements Excel spreadsheet, a tab is labeled User Stories. No response is required for Tab 3; these were provided to bidders for clarity and understanding of the expected journey a Constituent will experience.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Tyler
DATE: 6/11/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

☒ P, Q, N or I Notes:P Addition of Okta to eliminate password	**1. System security components System security must include the following security components:**
	1) Account Take Over Protections
	a) Account Sign-in Protections
	a) Account Sign-in Protections
	a) Adaptive AI Technology
	b) Bot Protection: identify visitor behavior through analysis of technical and behavioral data.
☒ P, Q, N or I Notes: P has 3 levels of identity, does have imaging and coupled with email	**2. Identity Proofing must have the ability to provide levels of proofing which will be directly tied to the constituent's level of access.**
	1) Define various levels of id proofing
	2) Document Image Capture
	3) Close coupling with authentication
☒ P, Q, N or I Notes: P Supports MFA	**3. Multi-factor authentication The system must support multi-factor authentication to protect against user impersonation and credential theft.**
☒ P, Q, N or I Notes: P, Uses Okta and a custom Tyler Identity	**4. Risk-based factors The system must support risk-based factors and scores that are based on factors such as, but not limited to, device and location.**
☒ P, Q, N or I Notes: P Missing a	**5. Identity lifecycle management components The system must include the following identity lifecycle management components for risk-based critical applications not**

description of off boarding	**limited to end users but also for generic accounts and system/service accounts:**
P	1) Identity Creation
P	2) Identity provisioning
P	3) Attribute maps
P	4) Authentication (e.g., password policies and synchronization)

☒ P, Q, N or I Notes: P.	**6. Security event logging The system must log security information and events.**
	Security Information and Event Management (SIEM) – Splunk
	Cloud Services: Azure, AWS, Oracle, Google
☒ P, Q, N or I Notes:P	**7. Security Certifications The system must comply too or have the following security certifications:**
Certified	1) NIST 800-53
Comply	2) FedRamp
Comply	3) HIPAA
Comply	4) SOC 2 Type II
	Note:
	IRS require a 45-day letter approval for new cloud solutions.
☒ P, Q, N or I Notes:P Will integrate	**8. SIEM (Splunk) integration The system must be able to integrate with the State of Maine Security Information and Event Monitoring (SIEM) Splunk for Security Operations Center operations.**
☒ P, Q, N or I	**9. Core constituent data. The system must maintain a central repository of basic (core) constituent data, that can be used by any SoM application to reduce data redundancy**

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Tyler
DATE: 6/11/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

Notes:P will be with constituents concent	**and outdated or inaccurate information while maintaining confidentiality.**
☒ P, Q, N or I Notes:	**11. Data Management. The system must apply the Data Management Rules to the constituent profile data as per the SoM Data Management Policies.**
☒ P, Q, N or I Notes:P agree to meet	**12. SOM Employee. The system must support multiple identities for SOM employees that work with the portal in a support role.**
P	1) SOM Employee identity and credentials for supporting the application.
P	2) Constituent identity and credentials to use the state services offered through the portal.

☒ P, Q, N or I Notes:P Use of Resident Engagement platform is interesting to keep coding to minimum	**13. APIs. The system must be able to connect to at least one agency application.**
	Considerations:
	a) OpenID, OAuth, WS-Fed, SAML, LDAP, Active Directory, Application Programming Interfaces (APIs), Software Development
	b) Develop once and reuse often with other agencies would be ideal
☒ P, Q, N or I Notes:P Willing to build a	**14. User identification matching. The system must be able to match the identity of the portal user to the identity of the same user in the agency system.**

verification server for agencies that don't have one.	
☒ P, Q, N or I Notes:P	**15. Single sign-on. The system must support single sign-on to the agency application.**
☒ P, Q, N or I Notes:P will need to build	**16. Import user profile data from agency systems. The system must be able to import user data from different SoM applications to ensure offboarding happens in a timely manner, so that government resources are protected from fraud. (example: death records)**
☒ P, Q, N or I Notes:P	**17. History logging.** 1) The system must log all actions taken by:
P	a) Constituents
P	b) MaineIT support
P	Including but not limited to:
P	c) who made the change
P	d) when the change was made
P	e) what changed
☒ P, Q, N or I Notes:P	**18. Reporting. The logging data (history) must be available for constituent and system dashboards and reporting in general.**
☒ P, Q, N or I Notes:P	**19. Security Controls. The system must comply to the following security controls:**
P	1) DDOS Protections[WN1] ,
P	2) OWASP Top 10
P	a) Cross Site Scripting,
P	b) SQL Injection,
P	3) Authentication bypass,
P	a) poorly authenticated APIs,
P	b) Role based access controls,

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Tyler
DATE: 6/11/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

P	c) proper session control
P	4) Real-time visibility,
P	5) Anomalous behavior,
P	6) User sign with geo-location tracking,
P	Geo-blocking capabilities.
P	Security controls must include Web Application Firewall [WN1]
☒ P, Q, N or I Notes:P	**20. General System Requirements.** 1) Mobile Support with Native App; (iOS and Android)
P	2) System availability: 24/7 with 4x1-hour outages per year
P	3) Identity relationships must be tracked in the cloud infrastructure.
P	4) Support responsive web and web browsers.
P	a. Supports Windows, Chrome, and Macintosh operating systems
☒ P, Q, N or I Notes:P	**21. Training and Support.** 1) Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
P	2) MaineIT will require technical/administrator training. There will be initial training and on-going training as users are added.
P	3) Have a continuous process to ensure constituents that may have run into issues setting up accounts can have help 24/7.
☒ P, Q, N or I Notes:P	**22. Support Requirements** 1) The Bidder will provide support, and maintenance for the solution to begin immediately after receiving the State's official acceptance of the implemented solution.
P	2) Support and maintenance will be provided for the terms and duration specified in the contract.
P	3) The Bidder will address all questions and reported problems related to the technical and functional operation of the system.
P	4) The Bidder must provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours: 8:00 a.m. to 5:00 p.m. Eastern Standard Time.

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Tyler
DATE: 6/11/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

P	5) As part of the maintenance agreement, the Bidder will make all product releases and upgrades available to the State at no additional charge.
P	6) All release and upgrades shall be implemented and tested by the Bidder, outside of the normal operating hours of the State government.
P	7) User testing shall occur during normal State business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State government.
☒ P, Q, N or I Notes:P	**23. Hosting** Solution can comply with MaineIT remote hosting policies. a) Remote Hosting Policy http://maine.gov/oit/policies/RemoteHostingPolicy.pdf b) Hosting Customization Policy http://maine.gov/oit/policies/HostingCustomizationPolicy.pdf
☒ P, Q, N or I Notes:P	**24. Disaster Recovery** Proposed Solution can comply with MaineIT security requirements and remote hosting requirements, without requiring waivers, before contract finalization.
P	1) Maintaining an availability metric of ninety-nine-point nine percent (99.9%) of uptime
P	2) Ensuring the capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six hours (i.e., maximum data loss cannot exceed six (6) hours);
P	3) Ensuring a recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours;
P	4) Ensuring the hosting environment provides adequate capacity to ensure that, under ethernet connectivity to the client device, data inquiry/lookup response is within three (3) seconds, and data modification response is within five (5) seconds;
P	5) Providing the Department at least thirty (30) calendar day advance written notice of any material change in network operations or architecture;
P	6) Ensuring any planned material change in network operations or architecture cannot be made without the prior written consent of the Department; and Outlining of all Service Level Agreements (SLAs) for technical support (the awarded Bidder

	shall be open to negotiation to ensure the SLAs meet the Department's needs

3. Response to Proposed Services (App. H - RFP pgs. 8-14)

☒1a) Bidders shall provide a full description of the proposed solution(s) detailed in Part II services to be provided.
P, N, Q, or I & Notes:

☒1b) Detailed description of the technologies, software and / or hardware for each of the components.
P, N, Q, or I & Notes:P

☒1c) Overview of the features and functions being proposed and why the proposed solution is best for the State.
P, N, Q, or I & Notes:P

☒1d) Description of the overall platform and architecture of the proposed solution(s).
P, N, Q, or I & Notes:P

☒1e) Description of any third-party software or partnerships required for the proposed Solution(s).
P, N, Q, or I & Notes:P

☒2a) A detailed timeline and description of milestones, deliverables, tasks
P, N, Q, or I & Notes:P

☒2b) A Resource Plan with resumes, roles and responsibilities (Identifying them as Vendor Staff (V), Contracted Staff (C), and/or State Staff (S)) Through

Implementation Period and Post Implementation – Support period
P, N, Q, or I & Notes:P

☒2c) Realistic detailed work plan for the implementation through the first contract period including details on deliverables to be installed or implemented.
P, N, Q, or I & Notes:P

☒2d) Average time to market for each component.
P, N, Q, or I & Notes:P

B.1. The State is seeking an Enterprise Constituent Identity Access Management (CIAM) solution to become a part of the State's, MaineIT Enterprise Architecture. The proposed CIAM Solution needs to include tiered identity proofing, which verifies the authenticity of an individual's identity claim, and identity verification, which confirms the accuracy of the provided information. The proposed CIAM solution must:

a. ☒Capture Constituent Identity and profile data.
   P, N, Q, or I & Notes:P
b. ☒Provide identity provisioning and deprovisioning.
   P, N, Q, or I & Notes:P
c. ☒Include a process for the following identity lifecycle management components for risk-based critical applications not limited to end user accounts:
   i. Identity Creation
   ii. Identity provisioning
   iii. Attribute maps
   iv. Authentication (e.g., password policies and synchronization)
      P, N, Q, or I & Notes:P
d. ☒Allow integration with applications across various State Agencies. More specifically, be capable of integrating with existing identity-proofing methods currently utilized by State Agencies.
   P, N, Q, or I & Notes:P
e. ☒Be able to integrate with authoritative sources of identity-proofing maintained by the State Agencies. No replication allowed.
   P, N, Q, or I & Notes:P
f. ☒Describe the extensibility of architecture so that future means of identity-

proofing (e.g. biometrics) may be incorporated.
P, N, Q, or I & Notes:P Using Socure

g. ☒Allow for multiple role selections for the following identities:
    i. Individual
    ii. Business Owner
    iii. Support multiple identities for State employees that work with the portal in a support role:
        (a) SOM Employee identity and credentials for supporting the application.
        (b) Constituent identity and credentials to use the state services offered through the portal.
    iv. Multi role individual (Individual and Business Owner)
    P, N, Q, or I & Notes:P

h. ☒Have the ability to provide levels of proofing which will be directly tied to the Constituent's level of consent given.
P, N, Q, or I & Notes:P

i. ☒Support multi-factor authentication to protect against user impersonation and credential theft.
P, N, Q, or I & Notes:P

B.2. ☒The State is seeking to improve Citizen satisfaction by implementing a Constituent centralized platform that will aim to provide Constituents with a one-stop-shop for accessing government services. While State Agencies continue to make advances in expanding their service offerings. The goal of the Personalized Dashboard (portal) is to change from Constituents searching to find State services, to one where the portal allows Constituents to choose State services to be included in their personalized dashboard. The portal will allow interaction to occur anytime or anywhere, allowing the Constituent a personalized dashboard into state services.
P, N, Q, or I & Notes:P

a. Disclosure and Consent Management

The desire of the State is to be as transparent as possible and respect the privacy of the individual interacting with the Constituents' Portal. Consent is a core tenant of maintaining the public trust in the Constituents' Portal and will be a foundational component of the architecture.

The Disclosure and Consent Management solution shall include:

- i. ☒Granular consent management that encompasses the automated functions necessary to create, modify, revoke, and manage Constituent consents.
- ii. ☒Allow users the ability to opt-in and opt-out of data sharing and services within the Constituents' portal.
- iii. ☒Obtain user consent both in an interactive and set preference mode for a variety of transactions on the Portal.
- iv. ☒Support administrative users' management of standard legal disclaimers and data classification for transactions.
- v. ☒Highly configurable with version control and history tracking for consent language.
- vi. ☒Ability for end user to access a retrievable log of granted consent and data usage on the portal derived from the consent.

P, N, Q, or I & Notes:

b. Recommendation Technology

The State is seeking options which, while maintaining individual privacy, will collect and analyze data about user interactions, behavior, and preferences. The expected outcome of this will be to provide insights and intelligence that help the State make informed decisions and improve Constituent experiences.

- i. ☒From the user perspective, the portal should be able to make real-time recommendations for related services.
- ii. ☒Data captured in this environment must be obfuscated, as to not allow any party to directly target or track the preferences of an individual or their usage of the portal.
- iii. ☒Solution providers should discuss in detail their use, storage, destruction of metadata, and tracking technologies with emphasis on how their offering provides analytical insights while protecting the individual user privacy.

P, N, Q, or I & Notes:P

c. Data Management

The State is seeking the ability for the portal's Constituent identity to be linked to records maintained by individual State agencies. The proposed solution will include:

- i. ☒Capabilities to streamline the sharing of data between State systems,

including
- i. The identity assurance level
- ii. Agency to user notifications
- iii. Verification of user consent
- iv. Identity resolution
- v. Data sharing between agencies.

ii. ☒Maintain a central repository of basic (core) Constituent data, that can be used by any State application to reduce data redundancy, and outdated or inaccurate information while maintaining confidentiality.

iii. ☒Ability to integrate with State applications using, OpenID, OAuth, Web Services Federation Protocol (WS-Fed), Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), Active Directory, Application Programming Interface (API) or equivalent protocols.

iv. ☒Ability to match the identity of the portal user to the identity of the same user in the Agency system.

v. ☒Log all actions taken by:
- i. Constituents
- ii. MaineIT Support, including:
  - (a) Who made the change
  - (b) When the change was made
  - (c) What changed to and from

vi. ☒Logging data must be available for system dashboards and reporting.

P, N, Q, or I & Notes:P

d. Customer Service

The State is seeking solution(s) to provide 24/7/365 customer service to Constituents regardless of their location or technical abilities.
- i. ☒Support Constituents with personalized and timely assistance.
- ii. ☒Provide the state options to support our Constituents across multiple channels including, but not limited to phone, email, chat, etc.

P, N, Q, or I & Notes: P

C.1. General System
- a. ☒Mobile support with native app (iOS and Android)
- b. ☒System availability: 24/7 with a maximum of four (4) 1-hour outages per year

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES

RFP #: 202401005
RFP TITLE: IMPROVE DELIVERY OF DIGITAL SERVICES TO CONSTITUENTS
BIDDER NAME: Tyler
DATE: 6/11/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: MaineIT

c. ☒Identity relationships must be tracked in the cloud infrastructure.
d. ☒Support responsive web and web browsers.
  i. ☒Supports Windows, Chrome, and Macintosh operating systems.

P, N, Q, or I & Notes:P

C.2. ☒Compliance with MaineIT Policies & Standards
a. Architecture Compliance Policy
b. System and Services Acquisition Policy and Procedures (SA-1)
c. Application Deployment Certification Policy
d. Digital Accessibility Policy
e. Remote Hosting Policy
f. Data Exchange Policy
g. Information Security Policy
h. Access Control Policy (AC-1)
i. Access Control Procedures for Users (AC-2)
j. Risk Assessment Policy and Procedures (RA-1)
k. Vulnerability Scanning Procedure (RA-5)
l. Security Assessment and Authorization Policy and Procedures (CA-1)
m. System and Information Integrity Policy and Procedures (SI-1)
n. Configuration Management Policy (CM-1)
o. Web Standards

P, N, Q, or I & Notes:P

C.3. Support and Maintenance
a. ☒Provide support and maintenance for the solution and underlying technology to begin immediately after receiving the State's official acceptance of the implemented solution.
P, N, Q, or I & Notes:P
b. ☒Terms and duration of the support and maintenance will be specified in the contract.
P, N, Q, or I & Notes:P

c. ☒All questions and reported problems related to the technical and functional operation of the system will be addressed by the awarded bidder.
P, N, Q, or I & Notes:P

d. ☒Provide toll-free telephone support through a qualified technician with direct and demonstrated experience in the implementation and maintenance of the approved implemented solution during regular business hours (8:00 a.m. to 5:00 p.m. EST)
P, N, Q, or I & Notes:P

e. ☒All product releases and upgrades available will be the responsibility of the awarded bidders, at no additional charge to the State.
P, N, Q, or I & Notes:P

f. ☒All releases and upgrades shall be implemented and tested by the bidder, outside of the normal operating hours of the State.
P, N, Q, or I & Notes:P

g. ☒User testing shall occur during normal state business hours. All remediation of failed testing cases and protocols shall also occur outside of the normal operating hours of the State.
P, N, Q, or I & Notes:P

4. Security

The proposed solutions must provide a robust security system that aligns with the States Security Policies, standards, and Processes, Including:

Comply with or have the following security certifications:

i. ☒National Institute of Standards and Technology (NIST) 800-53
ii. ☒FedRamp
iii. ☒Health Insurance Portability and Accountability Act (HIPAA)
iv. ☒SOC 2 Type II
v. ☒Comply to the following security controls:
vi. ☒DDOS Protections [WN1]
vii. ☒Open Web Application Security Project (OWASP) Top 10
viii. ☒Cross Site Scripting
ix. ☒Structured Query Language (SQL) Injection
x. ☒Authentication bypass
xi. ☒Poorly authenticated APIs
xii. ☒Role based access controls
xiii. ☒Proper session control
xiv. ☒Real-time visibility
xv. ☒Anomalous behavior
xvi. ☒User sign with geo-location tracking

xvii. ☒Geo-blocking capabilities.
xviii. ☒Web Application Firewall [WN1]
xix. ☒System security must include the following security components:
xx. ☒Account take over protections
xxi. ☒Account sign-in Protections
xxii. ☒Behavior detection and evaluation
xxiii. ☒Adaptive AI Technology
xxiv. ☒Bot Protection; identity visitor behavior through analysis, technical and behavioral data.
xxv. ☒The proposed solution must be able to integrate with the State Security Information and Event Monitoring (SIEM) Splunk. Ability to log security information and events.

P, N, Q, or I & Notes:P

5. Licensing

☒The State is aware that multiple licensing options are available and will be required to support the proposed solution in its entirety. The State seeks bids which will provide the most cost-effective licensing approach. Bidders are required to provide a detail breakdown for the proposed licensing.

P, N, Q, or I & Notes:P

1. Training and OCM (Organizational Change Management)

a. ☒Security, identity and access management, and application training must be provided to relevant staff for deployment and ongoing training to support the solution.
b. ☒Training must include technical and administrator training, initial and ongoing as users are added.
c. ☒Continuous process to ensure Constituents that may have run into issues setting up accounts have help 24/7.
d. ☒Bidders shall guide the State in OCM engagement for the duration of project planning, transition, and final implementation phase including:
   i. Designing and managing team structures with roles and responsibilities to facilitate automated program delivery, while noting any risks anticipated from the lack of readiness in the organization and staffing.
   ii. Ensure a successful transition for the integration of new processes and

technology with stakeholders.

iii. Organizational readiness assessment

P, N, Q, or I & Notes:P

3. Disaster Recovery

a. ☒Availability of ninety-nine-point nine percent (99.9%) of uptime

b. ☒Capability to restore data completely to its status at the time of the last backup; with a minimum required recovery point objective of six (6) hours (i.e., maximum data loss cannot exceed six (6) hours)

c. ☒Recovery time objective of two (2) hours; maximum time to recover the system cannot exceed 2 (2) hours.

P, N, Q, or I & Notes:P

4. Feature Enhancements

a. ☒The State is seeking two hundred and fifty (250) hours of time and material for each proposed technology (CIAM), Personalized Dashboard, Disclosure and Consent Management, Data Management, and Recommendation Technology) to allow for specifications and enhancements during the contract period.

P, N, Q, or I & Notes:P

5. Project Management

a. ☒The State plans to have its own project manager however, the awarded Bidder must have a project manager that has the primary responsibility for executing the project management tasks associated with the project. The awarded Bidder will:
   i. Work in collaboration with the State's Project Manager
   ii. Align with State Project Management processes and practices.

b. ☒Manage the implementation, executing all activities, tasks, deliverables and resource needs, both state and awarded Bidder.

c. ☒Track project status including managing and tracking all project risks, issues and decisions.

d. ☒Track and report status of deliverables and project status

e. ☒The awarded Bidder will provide their approach for project management and administration services including:

i. Project Management Methodology
ii. Project Governance
iii. Resource Allocation and Schedule Management approach
iv. Communication Management Approach including status reporting and document repository management.
v. Risk and Issue Management Methodology
vi. Change Management Methodology
vii. Quality Management Methodology

P, N, Q, or I & Notes:P

D. Value Added Options (Other)

☒Bidders shall provide value added optional services to address relevant matters that have not been anticipated in this RFP but contribute to successful implementation of the proposed solutions, as well as any technology or services that will reduce risk to the project's quality and continuity. The value-added technology and services will not be included in the evaluation process but may be added during the contract negotiations.

P, N, Q, or I & Notes:P. Push notifications, Calendar feeds, Maps and Surveys

Technical Assessment Consensus Notes

STATE OF MAINE
CONSENSUS EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Active Cyber
DATE: 16 May 2024
EVALUATOR NAME: CONSENSUS
EVALUATOR DEPARTMENT: DAFS-OIT

Does Not Meet Technical Requirements
Data Compliance
NIST 800-171: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
Maine FOAA: *Adequate response. Weak (missing) evidence.*
Maine Breach Notification Law: *Adequate response. Weak (missing) evidence.*
NIST 800-53: Rev5: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
Non-Functional Requirements
H1: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
H2: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
H3: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
A1: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
A2: *Adequate response. Weak evidence (The “our” is NOT the Prime’s, but copy-paste of Okta! And, does NOT cover ID.me).*
A3: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
A4: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
Information Security Standards
S1: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
S2: *Adequate response. Weak evidence (Covers Prime & Okta, NOT ID.me).*
S3: *Adequate response. Weak evidence (No specific detail).*
S4: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
S5: *Weak response. Weak evidence (Only covers Okta, NOT ID.me).*
Cloud Service Provider Requirements
CSP1: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
CSP2: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
CSP3: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
CSP4: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
CSP5: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
CSP6: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
CSP7: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
CSP8: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
CSP9: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
CSP10: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
CSP11: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
CSP12: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
CSP13: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
CSP14: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
NIST Requirement

STATE OF MAINE
CONSENSUS EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Active Cyber
DATE: 16 May 2024
EVALUATOR NAME: CONSENSUS
EVALUATOR DEPARTMENT: DAFS-OIT

N1: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
N2: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
N3: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
N4: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
N5: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
N6: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
N7: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
N8: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
N9: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
N10: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
N11: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
N12: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
N13: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
N14: *Not Applicable*

STATE OF MAINE
CONSENSUS EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Carahsoft
DATE: 16 May 2024
EVALUATOR NAME: CONSENSUS
EVALUATOR DEPARTMENT: DAFS-OIT

Does Not Meet Technical Requirements
Data Compliance
NIST 800-171: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
Maine FOAA: *Weak response. Weak (missing) evidence.*
Maine Breach Notification Law: *Adequate response. Weak (missing) evidence.*
NIST 800-53: Rev5: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
Non-Functional Requirements
H1: *Adequate response. Weak evidence (Only covers Ping, NOT Adobe, NOT OneTrust, NOT Publicis Sapient).*
H2: *Adequate response. Weak evidence (Only covers Ping, NOT Adobe, NOT OneTrust, NOT Publicis Sapient).*
H3: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
A1: *Adequate response. Weak evidence (Only covers Ping, NOT Adobe, NOT OneTrust, NOT Publicis Sapient).*
A2: *Adequate response. Weak evidence (No specific details).*
A3: *Adequate response. Weak evidence (Only covers Adobe, NOT Ping, NOT OneTrust, NOT Publicis Sapient).*
A4: Adequate *response. Weak evidence (No specific details).*
Information Security Standards
S1: *Weak response. Weak evidence (No specific details).*
S2: Adequate *response. Weak evidence (No specific details).*
S3: Adequate *response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
S4: *Adequate response (No specific details). Weak evidence (No specific details).*
S5: *Adequate response. Weak evidence (Cost Proposal).*
Cloud Service Provider Requirements
CSP1: Adequate *response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
CSP2: Adequate *response. Weak evidence (Only covers Adobe, NOT Ping, NOT OneTrust, NOT Publicis Sapient).*
CSP3: Adequate *response. Weak evidence (Only covers Adobe, NOT Ping, NOT OneTrust, NOT Publicis Sapient).*
CSP4: Adequate *response. Weak evidence (Only covers Adobe, NOT Ping, NOT OneTrust, NOT Publicis Sapient).*

STATE OF MAINE
CONSENSUS EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Carahsoft
DATE: 16 May 2024
EVALUATOR NAME: CONSENSUS
EVALUATOR DEPARTMENT: DAFS-OIT

CSP5: Adequate *response. Weak evidence (Only covers Adobe, NOT Ping, NOT OneTrust, NOT Publicis Sapient).*
CSP6: Adequate *response. Weak evidence (Only covers Adobe, NOT Ping, NOT OneTrust, NOT Publicis Sapient).*
CSP7: Adequate *response. Weak evidence (Only covers Adobe, NOT Ping, NOT OneTrust, NOT Publicis Sapient).*
CSP8: Adequate *response. Weak evidence (Only covers Adobe, NOT Ping, NOT OneTrust, NOT Publicis Sapient).*
CSP9: Adequate *response. Weak evidence (Only covers Adobe, NOT Ping, NOT OneTrust, NOT Publicis Sapient).*
CSP10: Adequate *response. Weak evidence (Only covers Adobe, NOT Ping, NOT OneTrust, NOT Publicis Sapient).*
CSP11: Adequate *response. Weak evidence (Only covers Adobe, NOT Ping, NOT OneTrust, NOT Publicis Sapient).*
CSP12: Adequate *response. Weak evidence (Only covers Adobe, NOT Ping, NOT OneTrust, NOT Publicis Sapient).*
CSP13: Adequate *response. Weak evidence (Only covers Adobe, NOT Ping, NOT OneTrust, NOT Publicis Sapient).*
CSP14: Adequate *response. Weak evidence (Only covers Adobe, NOT Ping, NOT OneTrust, NOT Publicis Sapient).*
NIST Requirement
N1: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
N2: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
N3: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
N4: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
N5: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
N6: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
N7: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
N8: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*

STATE OF MAINE
CONSENSUS EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Carahsoft
DATE: 16 May 2024
EVALUATOR NAME: CONSENSUS
EVALUATOR DEPARTMENT: DAFS-OIT

N9: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
N10: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
N11: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
N12: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
N13: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
N14: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*

STATE OF MAINE
CONSENSUS EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Deloitte
DATE: 16 May 2024
EVALUATOR NAME: CONSENSUS
EVALUATOR DEPARTMENT: DAFS-OIT

Meets Technical Requirements
Data Compliance
NIST 800-171: *Adequate response. Adequate evidence.*
Maine FOAA: *Adequate response. Weak (missing) evidence.*
Maine Breach Notification Law: *Adequate response. Adequate evidence.*
NIST 800-53: Rev5: *Adequate response. Adequate evidence.*
Non-Functional Requirements
H1: *Adequate response. Weak evidence (Only Salesforce & Okta, NOT Socure ID+).*
H2: *Adequate response. Weak evidence (Only Salesforce & Okta, NOT Socure ID+).*
H3: *Adequate response. Weak evidence (Only Salesforce & Okta, NOT Socure ID+).*
A1: *Adequate response. Weak evidence (Only Salesforce & Okta, NOT Socure ID+).*
A2: *Weak response. Adequate evidence.*
A3: *Adequate response. Weak evidence (Only Salesforce & Okta, NOT Socure ID+).*
A4: *Adequate response. Weak evidence (Only Salesforce & Okta, NOT Socure ID+).*
Information Security Standards
S1: *Adequate response. Weak evidence (Only Salesforce & Okta, NOT Socure ID+).*
S2: Adequate *response. Weak evidence (No specific details).*
S3: *Adequate response. Weak evidence (Only Salesforce & Okta, NOT Socure ID+).*
S4: *Adequate response. Weak evidence.*
S5: *Adequate response. Adequate evidence.*
Cloud Service Provider Requirements
CSP1: *Adequate response. Adequate evidence.*
CSP2: *Adequate response. Adequate evidence.*
CSP3: *Adequate response. Adequate evidence.*
CSP4: *Adequate response. Adequate evidence.*
CSP5: *Adequate response. Adequate evidence.*
CSP6: *Adequate response. Adequate evidence.*
CSP7: *Adequate response. Adequate evidence.*
CSP8: *Adequate response. Adequate evidence.*
CSP9: *Adequate response. Adequate evidence.*

STATE OF MAINE
CONSENSUS EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Deloitte
DATE: 16 May 2024
EVALUATOR NAME: CONSENSUS
EVALUATOR DEPARTMENT: DAFS-OIT

CSP10: *Adequate response. Adequate evidence.*
CSP11: *Adequate response. Adequate evidence.*
CSP12: *Adequate response. Adequate evidence.*
CSP13: *Adequate response. Adequate evidence.*
CSP14: *Adequate response. Adequate evidence.*
NIST Requirement
N1: *Adequate response. Adequate evidence.*
N2: *Adequate response. Adequate evidence.*
N3: *Adequate response. Adequate evidence.*
N4: *Adequate response. Adequate evidence.*
N5: *Adequate response. Adequate evidence.*
N6: *Adequate response. Adequate evidence.*
N7: *Adequate response. Adequate evidence.*
N8: *Adequate response. Adequate evidence.*
N9: *Adequate response. Adequate evidence.*
N10: *Adequate response. Adequate evidence.*
N11: *Adequate response. Adequate evidence.*
N12: *Adequate response. Adequate evidence.*
N13: *Adequate response. Adequate evidence.*
N14: *N/A*

STATE OF MAINE
CONSENSUS EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Microsoft
DATE: 16 May 2024
EVALUATOR NAME: CONSENSUS
EVALUATOR DEPARTMENT: DAFS-OIT

Does Meet Technical Requirements
Data Compliance
NIST 800-171: *Strong response. Strong evidence.*
Maine FOAA: *Adequate response. Weak (missing) evidence.*
Maine Breach Notification Law: *Adequate response. Weak (missing) evidence.*
NIST 800-53: Rev5: *Strong response. Strong evidence.*
Non-Functional Requirements
H1: *Adequate response. Adequate evidence.*
H2: *Adequate response. Adequate evidence.*
H3: *Adequate response. Adequate evidence.*
A1: *Adequate response. Adequate evidence.*
A2: *Adequate response. Adequate evidence.*
A3: *Adequate response. Adequate evidence.*
A4: *Adequate response. Adequate evidence.*
Information Security Standards
S1: *Adequate response. Adequate evidence.*
S2: *Adequate response. Adequate evidence.*
S3: *Adequate response. Adequate evidence.*
S4: *Adequate response. Adequate evidence.*
S5: *Adequate response. Adequate evidence.*
Cloud Service Provider Requirements
CSP1: *Strong response. Strong evidence.*
CSP2: *Strong response. Strong evidence.*
CSP3: *Strong response. Strong evidence.*
CSP4: *Strong response. Strong evidence.*
CSP5: *Strong response. Strong evidence.*
CSP6: *Strong response. Strong evidence.*
CSP7: *Strong response. Strong evidence.*
CSP8: *Strong response. Strong evidence.*
CSP9: *Strong response. Strong evidence.*
CSP10: *Strong response. Strong evidence.*
CSP11: *Strong response. Strong evidence.*
CSP12: *Strong response. Strong evidence.*
CSP13: *Strong response. Strong evidence.*
CSP14: *Strong response. Strong evidence.*
NIST Requirement
N1: *Strong response. Strong evidence.*
N2: *Strong response. Strong evidence.*

STATE OF MAINE
CONSENSUS EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Microsoft
DATE: 16 May 2024
EVALUATOR NAME: CONSENSUS
EVALUATOR DEPARTMENT: DAFS-OIT

N3: *Strong response. Strong evidence.*
N4: *Strong response. Strong evidence.*
N5: *Strong response. Strong evidence.*
N6: *Strong response. Strong evidence.*
N7: *Weak response. Strong evidence.*
N8: *Strong response. Strong evidence.*
N9: *Strong response. Strong evidence.*
N10: *Strong response. Strong evidence.*
N11: *Strong response. Strong evidence.*
N12: *Strong response. Strong evidence.*
N13: *Strong response. Strong evidence.*
N14: *Strong response. Strong evidence.*

STATE OF MAINE
CONSENSUS EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: PruTech
DATE: 20 May 2024
EVALUATOR NAME: CONSENSUS
EVALUATOR DEPARTMENT: DAFS-OIT

Meets Technical Requirements
Data Compliance
NIST 800-171: *Adequate response. Weak evidence.*
Maine FOAA: *Adequate response. Weak evidence.*
Maine Breach Notification Law: *Adequate response. Weak evidence.*
NIST 800-53: Rev5: *Adequate response. Weak evidence.*
Non-Functional Requirements
H1: *Adequate response. Weak evidence (Covered Okta, NOT Thales).*
H2: *Adequate response. Adequate evidence.*
H3: *Adequate response. Weak evidence (especially, Thales).*
A1: *Adequate response. Adequate evidence.*
A2: *Adequate response. Adequate evidence.*
A3: *Weak response ("every possible effort", "times vary"). Adequate evidence.*
A4: *Adequate response. Adequate evidence.*
Information Security Standards
S1: *Adequate response. Adequate evidence.*
S2: *Adequate response. Adequate evidence.*
S3: *Adequate response. Weak evidence (Covered Thales, NOT Okta).*
S4: *Adequate response. Weak evidence (Covered Thales, NOT Okta).*
S5: *Adequate response. Adequate evidence.*
Cloud Service Provider Requirements
CSP1: *Adequate response. Adequate evidence.*
CSP2: *Adequate response. Adequate evidence.*
CSP3: *Adequate response. Adequate evidence.*
CSP4: *Adequate response. Weak evidence. (Covered Okta, NOT Thales)*
CSP5: *Adequate response. Adequate evidence.*
CSP6: *Adequate response. Adequate evidence.*
CSP7: *Adequate response. Adequate evidence.*
CSP8: *Adequate response. Adequate evidence.*
CSP9: *Adequate response. Weak evidence. (Covered Okta, NOT Thales)*
CSP10: *Adequate response. Adequate evidence.*
CSP11: *Adequate response. Adequate evidence.*
CSP12: *Adequate response. Adequate evidence.*
CSP13: *Adequate response. Adequate evidence.*
CSP14: *Adequate response. Adequate evidence.*
NIST Requirement
N1: *Adequate response. Adequate evidence.*
N2: *Adequate response. Adequate evidence.*

STATE OF MAINE
CONSENSUS EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: PruTech
DATE: 20 May 2024
EVALUATOR NAME: CONSENSUS
EVALUATOR DEPARTMENT: DAFS-OIT

N3: *Adequate response. Adequate evidence.*
N4: *Adequate response. Adequate evidence.*
N5: *Adequate response. Adequate evidence.*
N6: *Adequate response. Adequate evidence.*
N7: *Adequate response. Adequate evidence.*
N8: *Adequate response. Adequate evidence.*
N9: *Adequate response. Adequate evidence.*
N10: *Adequate response. Adequate evidence.*
N11: *Adequate response. Adequate evidence.*
N12: *Adequate response. Adequate evidence.*
N13: *Adequate response. Adequate evidence.*
N14: *N/A*

STATE OF MAINE
CONSENSUS EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Servos
DATE: 20 May 2024
EVALUATOR NAME: CONSENSUS
EVALUATOR DEPARTMENT: DAFS-OIT

Does Not Meet Technical Requirements
Data Compliance
NIST 800-171: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
Maine FOAA: *Adequate response. Weak (missing) evidence.*
Maine Breach Notification Law: *Adequate response. Weak (missing) evidence.*
NIST 800-53: Rev5: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
Non-Functional Requirements
H1: *Adequate response. Weak evidence (No specific details).*
H2: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
H3: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
A1: *Adequate response. Weak evidence (No specific details).*
A2: *Adequate response. Weak evidence (No specific details).*
A3: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
A4: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
Information Security Standards
S1: *Adequate response. Weak evidence (Missing “Data Security Addendum”).*
S2: *Adequate response. Weak evidence. (No specific details).*
S3: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
S4: *Adequate response. Weak evidence (No specific details).*
S5: *Adequate response. Weak evidence (No specific details).*
Cloud Service Provider Requirements
CSP1: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
CSP2: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
CSP3: *Weak response (Blank). Weak evidence (Covered ServiceNow, NOT ID.me).*
CSP4: *Weak response (Blank). Weak evidence (Covered ServiceNow, NOT ID.me).*
CSP5: *Weak response (Blank). Weak evidence (Covered ServiceNow, NOT ID.me).*
CSP6: *Weak response (Blank). Weak evidence (Covered ServiceNow, NOT ID.me).*
CSP7: *Weak response (Blank). Weak evidence (Covered ServiceNow, NOT ID.me).*
CSP8: *Weak response (Blank). Weak evidence (Covered ServiceNow, NOT ID.me).*
CSP9: *Weak response (Blank). Weak evidence (Covered ServiceNow, NOT ID.me).*
CSP10: *Weak response (Blank). Weak evidence (Covered ServiceNow, NOT ID.me).*
CSP11: *Weak response (Blank). Weak evidence (Covered ServiceNow, NOT ID.me).*
CSP12: *Weak response (Blank). Weak evidence (Covered ServiceNow, NOT ID.me).*

STATE OF MAINE
CONSENSUS EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Servos
DATE: 20 May 2024
EVALUATOR NAME: CONSENSUS
EVALUATOR DEPARTMENT: DAFS-OIT

CSP13: *Weak response (Blank). Weak evidence (Covered ServiceNow, NOT ID.me).*
CSP14: *Weak response (Blank). Weak evidence (Covered ServiceNow, NOT ID.me).*
NIST Requirement
N1: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
N2: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
N3: *Adequate response. Weak evidence (No specific details).*
N4: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
N5: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
N6: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
N7: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
N8: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
N9: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
N10: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
N11: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
N12: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
N13: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
N14: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*

STATE OF MAINE
CONSENSUS EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Tyler
DATE: 20 May 2024
EVALUATOR NAME: CONSENSUS
EVALUATOR DEPARTMENT: DAFS-OIT

Does Not Meet Technical Requirements
Data Compliance
NIST 800-171: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
Maine FOAA: *Adequate response. Adequate evidence.*
Maine Breach Notification Law: *Adequate response. Adequate evidence.*
NIST 800-53: Rev5: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
Non-Functional Requirements
H1: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
H2: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
H3: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
A1: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
A2: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
A3: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
A4: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
Information Security Standards
S1: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
S2: *Adequate response. Weak evidence. (No specific details.)*
S3: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
S4: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
S5: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
Cloud Service Provider Requirements
CSP1: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
CSP2: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*

STATE OF MAINE
CONSENSUS EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Tyler
DATE: 20 May 2024
EVALUATOR NAME: CONSENSUS
EVALUATOR DEPARTMENT: DAFS-OIT

CSP3: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
CSP4: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
CSP5: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
CSP6: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
CSP7: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
CSP8: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
CSP9: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
CSP10: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
CSP11: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
CSP12: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
CSP13: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
CSP14: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
NIST Requirement
N1: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
N2: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
N3: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
N4: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
N5: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
N6: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*

STATE OF MAINE
CONSENSUS EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Tyler
DATE: 20 May 2024
EVALUATOR NAME: CONSENSUS
EVALUATOR DEPARTMENT: DAFS-OIT

N7: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
N8: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
N9: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
N10: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
N11: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
N12: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
N13: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
N14: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*

Technical Assessment
Individual Notes

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Active Cyber
DATE: 5-14-2024
EVALUATOR NAME: Chris Johnson
EVALUATOR DEPARTMENT: SOS IS

Data Compliance
NIST 800-171: Strong/Weak
Maine FOAA: Weak/Weak
Maine Breach Notification Law: Adequate/Weak
NIST 800-53: Rev5: Strong/Weak
MaineIT
H1: *Strong/Strong*
H2: *Strong/Strong*
H3: *Strong/Weak (service desk?)*
A1: *Strong/Strong*
A2: *Strong/Strong*
A3: *Strong/Strong*
A4: *Strong/Adequate*
Information Security Standards
S1: *Strong/Weak (Maine policies?)*
S2: *Strong/Acceptable (CGS Romania only?)*
S3: *Strong/Weak (no indication of what compliance means nor reference to NDA)*
S4: *Strong/*
S5: *N/A (Are they required to provide SBOM for what underlies the IDaaS?)*
Cloud Service Provider Reqs
CSP1: Adequate/Adequate
CSP2: Strong/Strong
CSP3: *Strong/Strong*
CSP4: *Strong/Strong*
CSP5: Weak/Weak (OKTA remote access instead of remote hosting obligations)
CSP6: *Strong/Strong*
CSP7: *Strong/Strong*
CSP8: *Strong/Strong*
CSP9: *Strong/Strong*
CSP10: *Strong/Strong*
CSP11: *Strong/Strong*
CSP12: *Strong/Strong*
CSP13: *Strong/Strong*
CSP14: *Strong/Strong*
NIST Requirement
N1: *Strong/Strong*
N2: *Strong/Strong*
N3: *Strong/Strong*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Active Cyber
DATE: 5-14-2024
EVALUATOR NAME: Chris Johnson
EVALUATOR DEPARTMENT: SOS IS

N4: *Strong/Strong*
N5: *Strong/Strong*
N6: *Strong/Strong*
N7: *Strong/Strong*
N8: *Strong/Strong*
N9: *Strong/Strong*
N10: *Strong/Strong*
N11: *Strong/Strong*
N12: *Strong/Strong*
N13: *Strong/Strong*
N14: *N/A*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Active Cyber
DATE: 10 May 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: DAFS-OIT

Data Compliance
NIST 800-171: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
Maine FOAA: *Adequate response. Weak (missing) evidence.*
Maine Breach Notification Law: *Adequate response. Weak (missing) evidence.*
NIST 800-53: Rev5: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
MaineIT
H1: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
H2: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
H3: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
A1: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
A2: *Adequate response. Weak evidence (The "our" is NOT the Prime's, but copy-past of Okta! And, does NOT cover ID.me).*
A3: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
A4: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
Information Security Standards
S1: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
S2: *Adequate response. Weak evidence (Covers Prime & Okta, NOT ID.me).*
S3: *Adequate response. Weak evidence (No specific detail).*
S4: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
S5: *Weak response. Weak evidence (Only covers Okta, NOT ID.me).*
Cloud Service Provider Reqs
CSP1: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
CSP2: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
CSP3: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
CSP4: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
CSP5: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
CSP6: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
CSP7: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
CSP8: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
CSP9: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
CSP10: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
CSP11: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
CSP12: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
CSP13: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
CSP14: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
NIST Requirement
N1: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Active Cyber
DATE: 10 May 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: DAFS-OIT

N2: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
N3: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
N4: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
N5: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
N6: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
N7: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
N8: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
N9: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
N10: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
N11: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
N12: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
N13: *Adequate response. Weak evidence (Only covers Okta, NOT ID.me).*
N14: *Not Applicable*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: ACTIVE CYBER
DATE: 04/24/2024
EVALUATOR NAME: BEN HASCHALK
EVALUATOR DEPARTMENT: DAFS/OIT/ISO

Data Compliance
NIST 800-171: *Quality of Response? Quality of Evidence? Adequate / Adequate*
Maine FOAA: *Quality of Response? Quality of Evidence? Adequate / Adequate*
Maine Breach Notification Law: *Quality of Response? Quality of Evidence? Adequate / Adequate*
NIST 800-53: Rev5: *Quality of Response? Quality of Evidence? Adequate / Adequate*
MaineIT
H1: *Quality of Response? Quality of Evidence? Strong / Adequate*
H2: *Quality of Response? Quality of Evidence? Strong / Adequate*
H3: *Quality of Response? Quality of Evidence? Adequate / Adequate*
A1: *Quality of Response? Quality of Evidence? Strong / Adequate*
A2: *Quality of Response? Quality of Evidence? Strong / Adequate*
A3: *Quality of Response? Quality of Evidence? Adequate / Adequate*
A4: *Quality of Response? Quality of Evidence? Adequate / Adequate*
Information Security Standards
S1: *Quality of Response? Quality of Evidence? Strong / Adequate*
S2: *Quality of Response? Quality of Evidence? Adequate / Adequate*
S3: *Quality of Response? Quality of Evidence? Adequate / Adequate*
S4: *Quality of Response? Quality of Evidence? Adequate / Weak*
S5: *Quality of Response? Quality of Evidence? Weak / Weak*
Cloud Service Provider Reqs
CSP1: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP2: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP3: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP4: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP5: *Quality of Response? Quality of Evidence? Weak / Adequate*
CSP6: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP7: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP8: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP9: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP10: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP11: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP12: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP13: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP14: *Quality of Response? Quality of Evidence? Adequate / Adequate*
NIST Requirement
N1: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N2: *Quality of Response? Quality of Evidence? Adequate / Adequate*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: ACTIVE CYBER
DATE: 04/24/2024
EVALUATOR NAME: BEN HASCHALK
EVALUATOR DEPARTMENT: DAFS/OIT/ISO

N3: *Quality of Response? Quality of Evidence? Weak / Adequate*
N4: *Quality of Response? Quality of Evidence? Weak / Adequate*
N5: *Quality of Response? Quality of Evidence? Weak / Adequate*
N6: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N7: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N8: *Quality of Response? Quality of Evidence? Weak / Adequate*
N9: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N10: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N11: *Quality of Response? Quality of Evidence? Weak / Adequate*
N12: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N13: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N14: *Quality of Response? Quality of Evidence? N/A*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Active Cyber
DATE: 5/14/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: Department of Administrative Services

Data Compliance
NIST 800-171: *Quality of Response? Positive Quality of Evidence? Positive*
Maine FOAA: *Quality of Response? Positive Quality of Evidence? Questionable*
Maine Breach Notification Law: *Quality of Response? Positive Quality of Evidence? Questionable*
NIST 800-53: Rev5: *Quality of Response? Positive Quality of Evidence? Positive*
MaineIT
H1: *Quality of Response? Positive Quality of Evidence? Questionable*
H2: *Quality of Response? Positive Quality of Evidence? Positive*
H3: *Quality of Response? Positive Quality of Evidence? Questionable*
A1: *Quality of Response? Positive Quality of Evidence? Positive*
A2: *Quality of Response? Positive Quality of Evidence? Positive*
A3: *Quality of Response? Positive Quality of Evidence? Positive*
A4: *Quality of Response? Positive Quality of Evidence? Negative*
Information Security Standards
S1: *Quality of Response? Positive Quality of Evidence? Negative*
S2: *Quality of Response? Negative Quality of Evidence? Negative*
S3: *Quality of Response? Positive Quality of Evidence? Positive*
S4: *Quality of Response? Positive Quality of Evidence? Questionable*
S5: *Quality of Response? Questionable Quality of Evidence? Questionable*
Cloud Service Provider Reqs
CSP1: *Quality of Response? Positive Quality of Evidence? Questionable*
CSP2: *Quality of Response? Positive Quality of Evidence? Positive*
CSP3: *Quality of Response? Positive Quality of Evidence? Positive*
CSP4: *Quality of Response? Positive Quality of Evidence? Questionable*
CSP5: *Quality of Response? Positive Quality of Evidence? Positive*
CSP6: *Quality of Response? Positive Quality of Evidence? Positive*
CSP7: *Quality of Response? Positive Quality of Evidence? Positive*
CSP8: *Quality of Response? Positive Quality of Evidence? Positive*
CSP9: *Quality of Response? Positive Quality of Evidence? Positive*
CSP10: *Quality of Response? Positive Quality of Evidence? Positive*
CSP11: *Quality of Response? Positive Quality of Evidence? Questionable*
CSP12: *Quality of Response? Positive Quality of Evidence? Positive*
CSP13: *Quality of Response? Positive Quality of Evidence? Positive*
CSP14: *Quality of Response? Positive Quality of Evidence? Positive*
NIST Requirement
N1: *Quality of Response? Positive Quality of Evidence? Positive*
N2: *Quality of Response? Positive Quality of Evidence? Positive*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Active Cyber
DATE: 5/14/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: Department of Administrative Services

N3: *Quality of Response? Positive Quality of Evidence? Positive*
N4: *Quality of Response? Positive Quality of Evidence? Positive*
N5: *Quality of Response? Positive Quality of Evidence? Positive*
N6: *Quality of Response? Positive Quality of Evidence? Positive*
N7: *Quality of Response? Positive Quality of Evidence? Positive*
N8: *Quality of Response? Positive Quality of Evidence? Positive*
N9: *Quality of Response? Positive Quality of Evidence? Positive*
N10: *Quality of Response? Positive Quality of Evidence? Positive*
N11: *Quality of Response? Positive Quality of Evidence? Positive*
N12: *Quality of Response? Positive Quality of Evidence? Positive*
N13: *Quality of Response? Positive Quality of Evidence? Positive*
N14: *Quality of Response? Positive Quality of Evidence? Questionable*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Active Cyber
DATE: 05/06/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

Data Compliance
NIST 800-171: *Quality of Response? Adequate Quality of Evidence? Weak*
Maine FOAA: *Quality of Response? Weak Quality of Evidence? Weak*
Maine Breach Notification Law: *Quality of Response? Weak Quality of Evidence? Weak*
NIST 800-53: Rev5: *Quality of Response? Adequate Quality of Evidence? Weak*
MaineIT
H1: *Quality of Response? Adequate Quality of Evidence? Adequate*
H2: *Quality of Response? Adequate Quality of Evidence? Adequate*
H3: *Quality of Response? Adequate Quality of Evidence? Adequate*
A1: *Quality of Response? Adequate Quality of Evidence? Adequate*
A2: *Quality of Response? Adequate Quality of Evidence? Weak*
A3: *Quality of Response? Adequate Quality of Evidence? Strong*
A4: *Quality of Response? Quality Adequate of Evidence? Weak*
Information Security Standards
S1: *Quality of Response? Adequate Quality of Evidence? Adequate*
S2: *Quality of Response? Adequate Quality of Evidence? Weak*
S3: *Quality of Response? Weak Quality of Evidence? weak*
S4: *Quality of Response? Weak Quality of Evidence? weak*
S5: *Quality of Response? weak Quality of Evidence? weak*
Cloud Service Provider Reqs
CSP1: *Quality of Response? Adequate Quality of Evidence? Adequate*
CSP2: *Quality of Response? Adequate Quality of Evidence? Adequate*
CSP3: *Quality of Response? Weak Quality of Evidence? weak*
CSP4: *Quality of Response? Adequate Quality of Evidence? Adequate*
CSP5: *Quality of Response? Weak Quality of Evidence? Adequate*
CSP6: *Quality of Response? weak Quality of Evidence? weak*
CSP7: *Quality of Response? Adequate Quality of Evidence? weak*
CSP8: *Quality of Response? Adequate Quality of Evidence? Adequate*
CSP9: *Quality of Response? Adequate Quality of Evidence? weak*
CSP10: *Quality of Response? Weak Quality of Evidence? weak*
CSP11: *Quality of Response? weak Quality of Evidence? weak*
CSP12: *Quality of Response? Weak Quality of Evidence? weak*
CSP13: *Quality of Response? Weak Quality of Evidence? weak*
CSP14: *Quality of Response? Adequate Quality of Evidence? Adequate*
NIST Requirement
N1: *Quality of Response? Adequate Quality of Evidence? weak*
N2: *Quality of Response? Adequate Quality of Evidence?weak*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Active Cyber
DATE: 05/06/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

N3: *Quality of Response? Adequate Quality of Evidence? Weak*
N4: *Quality of Response? Adequate Quality of Evidence? Weak*
N5: *Quality of Response? Adequate Quality of Evidence? Weak*
N6: *Quality of Response? Adequate Quality of Evidence? Weak*
N7: *Quality of Response? Adequate Quality of Evidence? Weak*
N8: *Quality of Response? Adequate Quality of Evidence? Weak*
N9: *Quality of Response? Adequate Quality of Evidence? Weak*
N10: *Quality of Response? Adequate Quality of Evidence? Weak*
N11: *Quality of Response? Adequate Quality of Evidence? Weak*
N12: *Quality of Response? Adequate Quality of Evidence? Weak*
N13: *Quality of Response? Adequate Quality of Evidence? Weak*
N14: *Quality of Response? Adequate Quality of Evidence? Weak*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Carasoft
DATE: 5/14/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: Department of Administrative Services

Data Compliance
NIST 800-171: *Quality of Response? Questionable Quality of Evidence? Questionable*
Maine FOAA: *Quality of Response? Questionable Quality of Evidence? Questionable*
Maine Breach Notification Law: *Quality of Response? Questionable Quality of Evidence? Questionable*
NIST 800-53: Rev5: *Quality of Response? Questionable Quality of Evidence? Questionable*
MaineIT
H1: *Quality of Response? Positive Quality of Evidence? Positive*
H2: *Quality of Response? Positive Quality of Evidence? Positive*
H3: *Quality of Response? Questionable Quality of Evidence? Negative*
A1: *Quality of Response? Positive Quality of Evidence? Positive*
A2: *Quality of Response? Positive Quality of Evidence? Positive*
A3: *Quality of Response? Positive Quality of Evidence? Questionable*
A4: *Quality of Response? Positive Quality of Evidence? Positive*
Information Security Standards
S1: *Quality of Response? Questionable Quality of Evidence? Negative*
S2: *Quality of Response? Positive Quality of Evidence? Questionable*
S3: *Quality of Response? Positive Quality of Evidence? Questionable*
S4: *Quality of Response? Positive Quality of Evidence? Questionable*
S5: *Quality of Response? Positive Quality of Evidence? Questionable*
Cloud Service Provider Reqs
CSP1: *Quality of Response? Positive Quality of Evidence? Positive*
CSP2: *Quality of Response? Questionable Quality of Evidence? Questionable*
CSP3: *Quality of Response? Questionable Quality of Evidence? Questionable*
CSP4: *Quality of Response? Positive Quality of Evidence? Positive*
CSP5: *Quality of Response? Questionable Quality of Evidence? Questionable*
CSP6: *Quality of Response? Questionable Quality of Evidence? Questionable*
CSP7: *Quality of Response? Positive Quality of Evidence? Positive*
CSP8: *Quality of Response? Positive Quality of Evidence? Positive*
CSP9: *Quality of Response? Questionable Quality of Evidence? Questionable*
CSP10: *Quality of Response? Positive Quality of Evidence? Positive*
CSP11: *Quality of Response? Positive Quality of Evidence? Positive*
CSP12: *Quality of Response? Questionable Quality of Evidence? Questionable*
CSP13: *Quality of Response? Questionable Quality of Evidence? Questionable*
CSP14: *Quality of Response? Questionable Quality of Evidence? Questionable*
NIST Requirement

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Carasoft
DATE: 5/14/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: Department of Administrative Services

N1: *Quality of Response? Negative Quality of Evidence? Negative*
N2: *Quality of Response? Negative Quality of Evidence? Negative*
N3: *Quality of Response? Negative Quality of Evidence? Negative*
N4: *Quality of Response? Negative Quality of Evidence? Negative*
N5: *Quality of Response? Negative Quality of Evidence? Negative*
N6: *Quality of Response? Negative Quality of Evidence? Negative*
N7: *Quality of Response? Negative Quality of Evidence? Negative*
N8: *Quality of Response? Negative Quality of Evidence? Negative*
N9: *Quality of Response? Negative Quality of Evidence? Negative*
N10: *Quality of Response? Negative Quality of Evidence? Negative*
N11: *Quality of Response? Negative Quality of Evidence? Negative*
N12: *Quality of Response? Negative Quality of Evidence? Negative*
N13: *Quality of Response? Negative Quality of Evidence? Negative*
N14: *Quality of Response? Negative Quality of Evidence? Negative*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: CARASOFT
DATE: 04/26/2024
EVALUATOR NAME: BEN HASCHALK
EVALUATOR DEPARTMENT: DAFS/OIT/ISO

Data Compliance
NIST 800-171: *Quality of Response? Quality of Evidence? Weak / Weak*
Maine FOAA: *Quality of Response? Quality of Evidence? Weak / Weak*
Maine Breach Notification Law: *Quality of Response? Quality of Evidence? Adequate / Adequate*
NIST 800-53: Rev5: *Quality of Response? Quality of Evidence? Weak / Weak*
MaineIT
H1: *Quality of Response? Quality of Evidence? Adequate / Adequate*
H2: *Quality of Response? Quality of Evidence? Adequate / Adequate*
H3: *Quality of Response? Quality of Evidence? Weak / Weak*
A1: *Quality of Response? Quality of Evidence? Adequate / Adequate*
A2: *Quality of Response? Quality of Evidence? Adequate / Adequate*
A3: *Quality of Response? Quality of Evidence? Adequate / Weak*
A4: *Quality of Response? Quality of Evidence? Weak / Weak*
Information Security Standards
S1: *Quality of Response? Quality of Evidence? Weak / Weak*
S2: *Quality of Response? Quality of Evidence? Weak / Weak*
S3: *Quality of Response? Quality of Evidence? Weak / Weak*
S4: *Quality of Response? Quality of Evidence? Weak / Weak*
S5: *Quality of Response? Quality of Evidence? Weak / Adequate*
Cloud Service Provider Reqs
CSP1: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP2: *Quality of Response? Quality of Evidence? Weak / Weak*
CSP3: *Quality of Response? Quality of Evidence? Weak / Weak*
CSP4: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP5: *Quality of Response? Quality of Evidence? Weak / Weak*
CSP6: *Quality of Response? Quality of Evidence? Weak / Weak*
CSP7: *Quality of Response? Quality of Evidence? Weak / Weak*
CSP8: *Quality of Response? Quality of Evidence? Weak / Weak*
CSP9: *Quality of Response? Quality of Evidence? Weak / Weak*
CSP10: *Quality of Response? Quality of Evidence? Weak / Weak*
CSP11: *Quality of Response? Quality of Evidence? Adequate / Weak*
CSP12: *Quality of Response? Quality of Evidence? Weak / Weak*
CSP13: *Quality of Response? Quality of Evidence? Weak / Weak*
CSP14: *Quality of Response? Quality of Evidence? Weak / Weak*
NIST Requirement
N1: *Quality of Response? Quality of Evidence? Weak / Adequate*
N2: *Quality of Response? Quality of Evidence? Weak / Adequate*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: CARASOFT
DATE: 04/26/2024
EVALUATOR NAME: BEN HASCHALK
EVALUATOR DEPARTMENT: DAFS/OIT/ISO

N3: *Quality of Response? Quality of Evidence? Weak / Adequate*
N4: *Quality of Response? Quality of Evidence? Weak / Adequate*
N5: *Quality of Response? Quality of Evidence? Weak / Adequate*
N6: *Quality of Response? Quality of Evidence? Weak / Weak*
N7: *Quality of Response? Quality of Evidence? Weak / Adequate*
N8: *Quality of Response? Quality of Evidence? Weak / Adequate*
N9: *Quality of Response? Quality of Evidence? Weak / Weak*
N10: *Quality of Response? Quality of Evidence? Weak / Adequate*
N11: *Quality of Response? Quality of Evidence? Weak / Adequate*
N12: *Quality of Response? Quality of Evidence? Weak / Weak*
N13: *Quality of Response? Quality of Evidence? Weak / Adequate*
N14: *Quality of Response? Quality of Evidence? Weak / Weak*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Carahsoft
DATE: 5-14-2024
EVALUATOR NAME: Chris Johnson
EVALUATOR DEPARTMENT: SOS IS

Data Compliance
NIST 800-171: *Weak/Weak*
Maine FOAA: *Weak/Weak*
Maine Breach Notification Law: *Weak/Weak*
NIST 800-53: Rev5: *Weak/Weak*
MaineIT
H1: *Strong/Acceptable*
H2: *Strong/Weak*
H3: *Weak/Weak*
A1: *Weak/Weak*
A2: *Weak/Weak*
A3: *Weak/Weak*
A4: *Strong/Weak*
Information Security Standards
S1: *Weak/Weak*
S2: *Strong/Weak*
S3: *Weak/Weak (no notification expectation in response nor Adobe Inc. Resp. doc)*
S4: *Strong/Weak*
S5: *Strong/?? (no access to referenced cost proposal yet for licensing info)*
Cloud Service Provider Reqs
CSP1: *Acceptable/Acceptable*
CSP2: *Weak/Weak*
CSP3: *Weak/Acceptable*
CSP4: *Strong/Strong*
CSP5: *Weak/Weak*
CSP6: *Weak/Acceptable*
CSP7: *Weak/Weak*
CSP8: *Weak/Weak*
CSP9: *Weak/Weak*
CSP10: *Weak/Weak*
CSP11: *Strong/Acceptable*
CSP12: *Weak/Acceptable*
CSP13: *Weak/Weak*
CSP14: *Weak/Adequate*
NIST Requirement
N1: *Weak/Weak*
N2: *Weak/Weak*
N3: *Weak/Weak*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Carahsoft
DATE: 5-14-2024
EVALUATOR NAME: Chris Johnson
EVALUATOR DEPARTMENT: SOS IS

N4: *Weak/Weak*
N5: *Weak/Weak*
N6: *Weak/Weak*
N7: *Weak/Weak*
N8: *Weak/Weak*
N9: *Weak/Weak*
N10: *Weak/Weak*
N11: *Weak/Weak*
N12: *Weak/Weak*
N13: *Weak/Weak*
N14: *Weak/Weak*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Carasoft
DATE: 5/6/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

Data Compliance
NIST 800-171: *Quality of Response? Weak Quality of Evidence? weak*
Maine FOAA: *Quality of Response? weak Quality of Evidence? weak*
Maine Breach Notification Law: *Quality of Response? Weak Quality of Evidence? weak*
NIST 800-53: Rev5: *Quality of Response? weak Quality of Evidence? weak*
MaineIT
H1: *Quality of Response? Adequate Quality of Evidence? weak*
H2: *Quality of Response? Weak Quality of Evidence? weak*
H3: *Quality of Response? Weak Quality of Evidence? weak*
A1: *Quality of Response? Weak Quality of Evidence? weak*
A2: *Quality of Response? Weak Quality of Evidence? weak*
A3: *Quality of Response? Adequate Quality of Evidence? Adequate*
A4: *Quality of Response? Adequate Quality of Evidence? weak*
Information Security Standards
S1: *Quality of Response? Adequate Quality of Evidence? weak*
S2: *Quality of Response? weak Quality of Evidence? weak*
S3: *Quality of Response? Weak Quality of Evidence? weak*
S4: *Quality of Response? Weak Quality of Evidence? Weak*
S5: *Quality of Response? Adequate Quality of Evidence? Adequate*
Cloud Service Provider Reqs
CSP1: *Quality of Response? Weak Quality of Evidence? Adequate*
CSP2: *Quality of Response? weak Quality of Evidence? weak*
CSP3: *Quality of Response? Weak Quality of Evidence? weak*
CSP4: *Quality of Response? Adequate Quality of Evidence? weak*
CSP5: *Quality of Response? Weak Quality of Evidence? weak*
CSP6: *Quality of Response? weak Quality of Evidence? weak*
CSP7: *Quality of Response? weak Quality of Evidence? weak*
CSP8: *Quality of Response? weak Quality of Evidence? weak*
CSP9: *Quality of Response? weak Quality of Evidence? weak*
CSP10: *Quality of Response? weak Quality of Evidence? weak*
CSP11: *Quality of Response? weak Quality of Evidence? weak*
CSP12: *Quality of Response? weak Quality of Evidence? weak*
CSP13: *Quality of Response? weak Quality of Evidence? weak*
CSP14: *Quality of Response? weak of Evidence? weak*
NIST Requirement
N1: *Quality of Response? weak Quality of Evidence?weak*
N2: *Quality of Response? Weak Quality of Evidence? weak*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Carasoft
DATE: 5/6/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

N3: *Quality of Response? Weak Quality of Evidence? weak*
N4: *Quality of Response? Weak Quality of Evidence? weak*
N5: *Quality of Response? Weak Quality of Evidence? weak*
N6: *Quality of Response? Weak Quality of Evidence? weak*
N7: *Quality of Response? Weak Quality of Evidence? weak*
N8: *Quality of Response? Weak Quality of Evidence? weak*
N9: *Quality of Response? weak Quality of Evidence? weak*
N10: *Quality of Response? weak Quality of Evidence? weak*
N11: *Quality of Response? weak Quality of Evidence? weak*
N12: *Quality of Response? weak Quality of Evidence? weak*
N13: *Quality of Response? weak Quality of Evidence? weak*
N14: *Quality of Response? weak Quality of Evidence? weak*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Carahsoft
DATE: 10 May 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: DAFS-OIT

Data Compliance
NIST 800-171: *Weak response (“P” for Partial?). Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
Maine FOAA: *Weak response (“P” for Partial?). Weak (missing) evidence.*
Maine Breach Notification Law: *Adequate response (“P” for Partial?). Weak (missing) evidence.*
NIST 800-53: Rev5: *Weak response (“P” for Partial?). Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
MaineIT
H1: *Adequate response. Weak evidence (Only covers Ping, NOT Adobe, NOT OneTrust, NOT Publicis Sapient).*
H2: *Adequate response. Weak evidence (Only covers Ping, NOT Adobe, NOT OneTrust, NOT Publicis Sapient).*
H3: *Weak response (“P” for Partial?). Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
A1: *Adequate response. Weak evidence (Only covers Ping, NOT Adobe, NOT OneTrust, NOT Publicis Sapient).*
A2: *Adequate response. Weak evidence (No specific details).*
A3: *Adequate response. Weak evidence (Only covers Adobe, NOT Ping, NOT OneTrust, NOT Publicis Sapient).*
A4: Adequate *response. Weak evidence (No specific details).*
Information Security Standards
S1: *Weak response (“P” for Partial?). Weak evidence (No specific details).*
S2: Adequate *response. Weak evidence (No specific details).*
S3: Adequate *response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
S4: *Adequate response (No specific details). Weak evidence (No specific details).*
S5: *Adequate response. Adequate evidence (Cost Proposal).*
Cloud Service Provider Reqs
CSP1: Adequate *response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
CSP2: Adequate *response. Weak evidence (Only covers Adobe, NOT Ping, NOT OneTrust, NOT Publicis Sapient).*
CSP3: Adequate *response. Weak evidence (Only covers Adobe, NOT Ping, NOT OneTrust, NOT Publicis Sapient).*
CSP4: Adequate *response. Weak evidence (Only covers Adobe, NOT Ping, NOT OneTrust, NOT Publicis Sapient).*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Carahsoft
DATE: 10 May 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: DAFS-OIT

CSP5: Adequate *response. Weak evidence (Only covers Adobe, NOT Ping, NOT OneTrust, NOT Publicis Sapient).*
CSP6: Adequate *response. Weak evidence (Only covers Adobe, NOT Ping, NOT OneTrust, NOT Publicis Sapient).*
CSP7: Adequate *response. Weak evidence (Only covers Adobe, NOT Ping, NOT OneTrust, NOT Publicis Sapient).*
CSP8: Adequate *response. Weak evidence (Only covers Adobe, NOT Ping, NOT OneTrust, NOT Publicis Sapient).*
CSP9: Adequate *response. Weak evidence (Only covers Adobe, NOT Ping, NOT OneTrust, NOT Publicis Sapient).*
CSP10: Adequate *response. Weak evidence (Only covers Adobe, NOT Ping, NOT OneTrust, NOT Publicis Sapient).*
CSP11: Adequate *response. Weak evidence (Only covers Adobe, NOT Ping, NOT OneTrust, NOT Publicis Sapient).*
CSP12: Adequate *response. Weak evidence (Only covers Adobe, NOT Ping, NOT OneTrust, NOT Publicis Sapient).*
CSP13: Adequate *response. Weak evidence (Only covers Adobe, NOT Ping, NOT OneTrust, NOT Publicis Sapient).*
CSP14: Adequate *response. Weak evidence (Only covers Adobe, NOT Ping, NOT OneTrust, NOT Publicis Sapient).*
NIST Requirement
N1: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
N2: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
N3: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
N4: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
N5: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
N6: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
N7: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
N8: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Carahsoft
DATE: 10 May 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: DAFS-OIT

N9: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
N10: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
N11: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
N12: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
N13: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*
N14: *Weak response. Weak evidence (Only covers Adobe & Ping, NOT OneTrust, NOT Publicis Sapient).*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Deloitte
DATE: 5/15/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: Department of Administrative Services

Data Compliance
NIST 800-171: *Quality of Response? Positive Quality of Evidence? Positive*
Maine FOAA: *Quality of Response? Positive Quality of Evidence? Questionable*
Maine Breach Notification Law: *Quality of Response? Positive Quality of Evidence? Positive*
NIST 800-53: Rev5: *Quality of Response? Positive Quality of Evidence? Positive*
MaineIT
H1: *Quality of Response? Positive Quality of Evidence? Positive*
H2: *Quality of Response? Positive Quality of Evidence? Positive*
H3: *Quality of Response? Positive Quality of Evidence? Positive*
A1: *Quality of Response? Positive Quality of Evidence? Positive*
A2: *Quality of Response? Positive Quality of Evidence? Positive*
A3: *Quality of Response? Positive Quality of Evidence? Questionable*
A4: *Quality of Response? Positive Quality of Evidence? Questionable*
Information Security Standards
S1: *Quality of Response? Positive Quality of Evidence? Positive*
S2: *Quality of Response? Positive Quality of Evidence? Positive*
S3: *Quality of Response? Positive Quality of Evidence? Positive*
S4: *Quality of Response? Positive Quality of Evidence? Positive*
S5: *Quality of Response? Positive Quality of Evidence? Questionable*
Cloud Service Provider Reqs
CSP1: *Quality of Response? Positive Quality of Evidence? Positive*
CSP2: *Quality of Response? Positive Quality of Evidence? Positive*
CSP3: *Quality of Response? Positive Quality of Evidence? Positive*
CSP4: *Quality of Response Positive Quality of Evidence? Positive*
CSP5: *Quality of Response? Positive Quality of Evidence? Positive*
CSP6: *Quality of Response? Positive Quality of Evidence? Positive*
CSP7: *Quality of Response? Positive Quality of Evidence? Positive*
CSP8: *Quality of Response? Positive Quality of Evidence? Positive*
CSP9: *Quality of Response? Positive Quality of Evidence? Positive*
CSP10: *Quality of Response? Positive Quality of Evidence? Positive*
CSP11: *Quality of Response? Positive Quality of Evidence? Positive*
CSP12: *Quality of Response? Positive Quality of Evidence? Positive*
CSP13: *Quality of Response? Positive Quality of Evidence? Positive*
CSP14: *Quality of Response? Positive Quality of Evidence? Positive*
NIST Requirement
N1: *Quality of Response? Positive Quality of Evidence? Positive*
N2: *Quality of Response? Positive Quality of Evidence? Positive*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Deloitte
DATE: 5/15/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: Department of Administrative Services

N3: *Quality of Response? Positive Quality of Evidence? Positive*
N4: *Quality of Response? Positive Quality of Evidence? Positive*
N5: *Quality of Response? Positive Quality of Evidence? Positive*
N6: *Quality of Response? Positive Quality of Evidence? Positive*
N7: *Quality of Response? Positive Quality of Evidence? Positive*
N8: *Quality of Response? Positive Quality of Evidence? Positive*
N9: *Quality of Response? Positive Quality of Evidence? Positive*
N10: *Quality of Response? Positive Quality of Evidence? Positive*
N11: *Quality of Response? Positive Quality of Evidence? Positive*
N12: *Quality of Response? Positive Quality of Evidence? Positive*
N13: *Quality of Response? Positive Quality of Evidence? Positive*
N14: *Quality of Response? Negative Quality of Evidence? Negative*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: DELOITTE
DATE: 05/07/2024
EVALUATOR NAME: BEN HASCHALK
EVALUATOR DEPARTMENT: DAFS/OIT/ISO

Data Compliance
NIST 800-171: *Quality of Response? Quality of Evidence? Adequate / Adequate*
Maine FOAA: *Quality of Response? Quality of Evidence? Adequate / Adequate*
Maine Breach Notification Law: *Quality of Response? Quality of Evidence? Adequate / Adequate*
NIST 800-53: Rev5: *Quality of Response? Quality of Evidence? Adequate / Weak*
MaineIT
H1: *Quality of Response? Quality of Evidence? Adequate / Adequate*
H2: *Quality of Response? Quality of Evidence? Adequate / Adequate*
H3: *Quality of Response? Quality of Evidence? Adequate / Adequate*
A1: *Quality of Response? Quality of Evidence? Adequate / Adequate*
A2: *Quality of Response? Quality of Evidence? Adequate / Adequate*
A3: *Quality of Response? Quality of Evidence? Adequate / Adequate*
A4: *Quality of Response? Quality of Evidence? Adequate / Adequate*
Information Security Standards
S1: *Quality of Response? Quality of Evidence? Adequate / Adequate*
S2: *Quality of Response? Quality of Evidence? Adequate / Adequate*
S3: *Quality of Response? Quality of Evidence? Adequate / Adequate*
S4: *Quality of Response? Quality of Evidence? Adequate / Adequate*
S5: *Quality of Response? Quality of Evidence? Adequate / Adequate*
Cloud Service Provider Reqs
CSP1: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP2: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP3: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP4: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP5: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP6: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP7: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP8: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP9: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP10: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP11: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP12: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP13: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP14: *Quality of Response? Quality of Evidence? Adequate / Adequate*
NIST Requirement
N1: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N2: *Quality of Response? Quality of Evidence? Adequate / Adequate*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: DELOITTE
DATE: 05/07/2024
EVALUATOR NAME: BEN HASCHALK
EVALUATOR DEPARTMENT: DAFS/OIT/ISO

N3: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N4: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N5: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N6: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N7: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N8: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N9: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N10: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N11: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N12: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N13: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N14: *Quality of Response? Quality of Evidence? Adequate / Adequate*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Deloitte
DATE: 5-14-24
EVALUATOR NAME: Chris Johnson
EVALUATOR DEPARTMENT: SOS IS

Data Compliance
NIST 800-171: *Strong/Weak (No statement that Salesforce complies with 800-171, only Okta)*
Maine FOAA: *Strong/Weak*
Maine Breach Notification Law: *Strong/Weak (No referenced artifacts)*
NIST 800-53: Rev5: *Strong/Weak (No statement of SF/Okta compliance beyond Yes)*
MaineIT
H1: *Strong/Strong*
H2: *Strong/Strong*
H3: *Strong/Adequate*
A1: *Strong/Adequate*
A2: *Strong/Weak*
A3: *Adequate/Weak*
A4: *Weak/Weak*
Information Security Standards
S1: *Strong/Adequate*
S2: *Strong/Adequate*
S3: *Strong/Strong*
S4: *Weak/Weak*
S5: *Weak/Weak*
Cloud Service Provider Reqs
CSP1: *Strong/Strong*
CSP2: *Adequate/Strong*
CSP3: *Adequate/Strong*
CSP4: *Strong/Strong*
CSP5: *Strong/Strong*
CSP6: *Strong/Strong*
CSP7: *Strong/Strong*
CSP8: *Strong/Strong*
CSP9: *Strong/Strong*
CSP10: *Strong/Strong*
CSP11: *Strong/Strong*
CSP12: *Strong/Strong*
CSP13: *Strong/Strong*
CSP14: *Strong/Strong*
NIST Requirement
N1: *Weak/Weak (only part of solution is 800-53 rev 4 compliant?)*
N2: *Weak/Weak (No NIST references)*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Deloitte
DATE: 5-14-24
EVALUATOR NAME: Chris Johnson
EVALUATOR DEPARTMENT: SOS IS

N3: *Weak/Weak (No NIST references)*
N4: *Weak/Weak (No NIST references)*
N5: *Weak/Weak (only part of solution is 800-53 rev 4 compliant?)*
N6: *Weak/Weak (No NIST references)*
N7: *Strong/Strong*
N8: *Weak/Weak (No NIST references)*
N9: *Adequate/Weak (No NIST references)*
N10: *Weak/Weak (No NIST references or system protections)*
N11: *Weak/Weak (No NIST ref, sidesteps maintenance)*
N12: *Weak/Weak (No NIST ref, re own media protection)*
N13: *Weak/Weak (No NIST ref, sounds like no standard practice)*
N14: *N/A*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Deloitte
DATE: 05/06/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

Data Compliance
NIST 800-171: *Quality of Response? Adequate Quality of Evidence? Adequate*
Maine FOAA: *Quality of Response? weak Quality of Evidence? weak*
Maine Breach Notification Law: *Quality of Response? Adequate Quality of Evidence? Adequate*
NIST 800-53: Rev5: *Quality of Response? Adequate Quality of Evidence? Adequate*
MaineIT
H1: *Quality of Response? Strong Quality of Evidence? Strong*
H2: *Quality of Response? Strong Quality of Evidence? Adequate*
H3: *Quality of Response? Adequate Quality of Evidence? Adequate*
A1: *Quality of Response? Adequate Quality of Evidence? Adequate*
A2: *Quality of Response? Strong Quality of Evidence? Adequate*
A3: *Quality of Response? Adequate Quality of Evidence? Weak*
A4: *Quality of Response? Adequate Quality of Evidence? Adequate*
Information Security Standards
S1: *Quality of Response? Strong Quality of Evidence? Adequate*
S2: *Quality of Response? Adequate Quality of Evidence? Weak*
S3: *Quality of Response? Adequate Quality of Evidence? Adequate*
S4: *Quality of Response? Adequate Quality of Evidence? Weak*
S5: *Quality of Response? Adequate Quality of Evidence? Adequate*
Cloud Service Provider Reqs
CSP1: *Quality of Response? Strong Quality of Evidence? Strong*
CSP2: *Quality of Response? Adequate Quality of Evidence? Adequate*
CSP3: *Quality of Response? Adequate Quality of Evidence? Weak*
CSP4: *Quality of Response? Adequate Quality of Evidence? Adequate*
CSP5: *Quality of Response? Strong Quality of Evidence? Adequate*
CSP6: *Quality of Response? Strong Quality of Evidence? Adequate*
CSP7: *Quality of Response? Strong Quality of Evidence? Adequate*
CSP8: *Quality of Response? Strong Quality of Evidence? Adequate*
CSP9: *Quality of Response? Adequate Quality of Evidence? Adequate*
CSP10: *Quality of Response? Strong Quality of Evidence? Adequate*
CSP11: *Quality of Response? Adequate Quality of Evidence? Adequate*
CSP12: *Quality of Response? Adequate Quality of Evidence? Adequate*
CSP13: *Quality of Response? Adequate Quality of Evidence? Adequate*
CSP14: *Quality of Response? Adequate Quality of Evidence? Adequate*
NIST Requirement
N1: *Quality of Response? Strong Quality of Evidence? Adequate*
N2: *Quality of Response? Strong Quality of Evidence? Adequate*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Deloitte
DATE: 05/06/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

N3: *Quality of Response? Strong Quality of Evidence? Adequate*
N4: *Quality of Response? Adequate Quality of Evidence? weak*
N5: *Quality of Response? Adequate Quality of Evidence? Adequate*
N6: *Quality of Response? Adequate Quality of Evidence? Adequate*
N7: *Quality of Response? Adequate Quality of Evidence? Adequate*
N8: *Quality of Response? Strong Quality of Evidence? Adequate*
N9: *Quality of Response? Adequate Quality of Evidence? Adequate*
N10: *Quality of Response? Strong Quality of Evidence? Adequate*
N11: *Quality of Response? Adequate Quality of Evidence? Adequate*
N12: *Quality of Response? Adequate Quality of Evidence? Adequate*
N13: *Quality of Response? Adequate Quality of Evidence? Adequate*
N14: *Quality of Response? Na Quality of Evidence? na*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Deloitte
DATE: 10 May 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: DAFS-OIT

Data Compliance
NIST 800-171: *Adequate response. Adequate evidence.*
Maine FOAA: *Adequate response. Weak (missing) evidence.*
Maine Breach Notification Law: *Adequate response. Adequate evidence.*
NIST 800-53: Rev5: *Adequate response. Adequate evidence.*
MaineIT
H1: *Adequate response. Weak evidence (Only Salesforce & Okta, NOT Socure ID+).*
H2: *Adequate response. Weak evidence (Only Salesforce & Okta, NOT Socure ID+).*
H3: *Adequate response. Weak evidence (Only Salesforce & Okta, NOT Socure ID+).*
A1: *Adequate response. Weak evidence (Only Salesforce & Okta, NOT Socure ID+).*
A2: *Weak response. Adequate evidence.*
A3: *Adequate response. Weak evidence (Only Salesforce & Okta, NOT Socure ID+).*
A4: *Adequate response. Weak evidence (Only Salesforce & Okta, NOT Socure ID+).*
Information Security Standards
S1: *Adequate response. Weak evidence (Only Salesforce & Okta, NOT Socure ID+).*
S2: Adequate *response. Weak evidence (No specific details).*
S3: *Adequate response. Weak evidence (Only Salesforce & Okta, NOT Socure ID+).*
S4: *Adequate response. Adequate evidence.*
S5: *Adequate response. Adequate evidence.*
Cloud Service Provider Reqs
CSP1: *Strong response. Strong evidence.*
CSP2: *Strong response. Strong evidence.*
CSP3: *Strong response. Strong evidence.*
CSP4: *Strong response. Strong evidence.*
CSP5: *Strong response. Strong evidence.*
CSP6: *Strong response. Strong evidence.*
CSP7: *Strong response. Strong evidence.*
CSP8: *Strong response. Strong evidence.*
CSP9: *Strong response. Strong evidence.*
CSP10: *Strong response. Strong evidence.*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Deloitte
DATE: 10 May 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: DAFS-OIT

CSP11: *Strong response. Strong evidence.*
CSP12: *Strong response. Strong evidence.*
CSP13: *Strong response. Strong evidence.*
CSP14: *Strong response. Strong evidence.*
NIST Requirement
N1: *Strong response. Strong evidence.*
N2: *Strong response. Strong evidence.*
N3: *Strong response. Strong evidence.*
N4: *Strong response. Strong evidence.*
N5: *Strong response. Strong evidence.*
N6: *Strong response. Strong evidence.*
N7: *Strong response. Strong evidence.*
N8: *Strong response. Strong evidence.*
N9: *Strong response. Strong evidence.*
N10: *Strong response. Strong evidence.*
N11: *Strong response. Strong evidence.*
N12: *Strong response. Strong evidence.*
N13: *Strong response. Strong evidence.*
N14: *Strong response. Strong evidence.*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Microsoft
DATE: 5/15/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: Department of Administrative Services

Data Compliance
NIST 800-171: *Quality of Response? Positive Quality of Evidence? Positive*
Maine FOAA: *Quality of Response? Positive Quality of Evidence? Questionable*
Maine Breach Notification Law: *Positive Quality of Evidence? Positive*
NIST 800-53: Rev5: *Quality of Response? Positive Quality of Evidence? Positive*
MaineIT
H1: *Quality of Response? Positive Quality of Evidence? Positive*
H2: *Quality of Response? Positive Quality of Evidence? Positive*
H3: *Quality of Response? Positive Quality of Evidence? Positive*
A1: *Quality of Response? Positive Quality of Evidence? Positive*
A2: *Quality of Response? Positive Quality of Evidence? Positive*
A3: *Quality of Response? Positive Quality of Evidence? Positive*
A4: *Quality of Response? Positive Quality of Evidence? Positive*
Information Security Standards
S1: *Quality of Response? Positive Quality of Evidence? Positive*
S2: *Quality of Response? Positive Quality of Evidence? Positive*
S3: *Quality of Response? Positive Quality of Evidence? Positive*
S4: *Quality of Response? Positive Quality of Evidence? Positive*
S5: *Quality of Response? Positive Quality of Evidence? Positive*
Cloud Service Provider Reqs
CSP1: *Quality of Response? Positive Quality of Evidence? Positive*
CSP2: *Quality of Response? Positive Quality of Evidence? Positive*
CSP3: *Quality of Response? Positive Quality of Evidence? Positive*
CSP4: *Quality of Response? Positive Quality of Evidence? Positive*
CSP5: *Quality of Response? Positive Quality of Evidence? Positive*
CSP6: *Quality of Response? Positive Quality of Evidence? Positive*
CSP7: *Quality of Response? Positive Quality of Evidence? Positive*
CSP8: *Quality of Response? Positive Quality of Evidence? Positive*
CSP9: *Quality of Response? Positive Quality of Evidence? Positive*
CSP10: *Quality of Response? Positive Quality of Evidence? Positive*
CSP11: *Quality of Response? Positive Quality of Evidence? Positive*
CSP12: *Quality of Response? Positive Quality of Evidence? Positive*
CSP13: *Quality of Response? Positive Quality of Evidence? Positive*
CSP14: *Quality of Response? Positive Quality of Evidence? Positive*
NIST Requirement
N1: *Quality of Response? Positive Quality of Evidence? Positive*
N2: *Quality of Response? Positive Quality of Evidence? Positive*
N3: *Quality of Response? Positive Quality of Evidence? Positive*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Microsoft
DATE: 5/15/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: Department of Administrative Services

N4: *Quality of Response? Positive Quality of Evidence? Positive*
N5: *Quality of Response? Positive Quality of Evidence? Positive*
N6: *Quality of Response? Positive Quality of Evidence? Positive*
N7: *Quality of Response? Positive Quality of Evidence? Positive*
N8: *Quality of Response? Positive Quality of Evidence? Positive*
N9: *Quality of Response? Positive Quality of Evidence? Positive*
N10: *Quality of Response? Positive Quality of Evidence? Positive*
N11: *Quality of Response? Positive Quality of Evidence? Positive*
N12: *Quality of Response? Positive Quality of Evidence? Positive*
N13: *Quality of Response? Positive Quality of Evidence? Positive*
N14: *Quality of Response? Positive Quality of Evidence? Positive*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: MICROSOFT
DATE: 04/30/2024
EVALUATOR NAME: BEN HASCHALK
EVALUATOR DEPARTMENT: DAFS/OIT/ISO

Data Compliance
NIST 800-171: *Quality of Response? Quality of Evidence? Strong / Adequate*
Maine FOAA: *Quality of Response? Quality of Evidence? Adequate / Adequate*
Maine Breach Notification Law: *Quality of Response? Quality of Evidence? Adequate / Adequate*
NIST 800-53: Rev5: *Quality of Response? Quality of Evidence? Adequate / Adequate*
MaineIT
H1: *Quality of Response? Quality of Evidence? Adequate / Adequate*
H2: *Quality of Response? Quality of Evidence? Adequate / Adequate*
H3: *Quality of Response? Quality of Evidence? Adequate / Adequate*
A1: *Quality of Response? Quality of Evidence? Adequate / Adequate*
A2: *Quality of Response? Quality of Evidence? Adequate / Adequate*
A3: *Quality of Response? Quality of Evidence? Adequate / Adequate*
A4: *Quality of Response? Quality of Evidence? Adequate / Adequate*
Information Security Standards
S1: *Quality of Response? Quality of Evidence? Adequate / Adequate*
S2: *Quality of Response? Quality of Evidence? Adequate / Adequate*
S3: *Quality of Response? Quality of Evidence? Adequate / Adequate*
S4: *Quality of Response? Quality of Evidence? Weak / Weak*
S5: *Quality of Response? Quality of Evidence? Adequate / Adequate*
Cloud Service Provider Reqs
CSP1: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP2: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP3: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP4: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP5: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP6: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP7: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP8: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP9: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP10: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP11: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP12: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP13: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP14: *Quality of Response? Quality of Evidence? Adequate / Adequate*
NIST Requirement
N1: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N2: *Quality of Response? Quality of Evidence? Adequate / Adequate*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: MICROSOFT
DATE: 04/30/2024
EVALUATOR NAME: BEN HASCHALK
EVALUATOR DEPARTMENT: DAFS/OIT/ISO

N3: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N4: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N5: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N6: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N7: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N8: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N9: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N10: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N11: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N12: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N13: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N14: *Quality of Response? Quality of Evidence? Adequate / Adequate*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Microsoft Corporation
DATE: 5-14-24
EVALUATOR NAME: Chris Johnson
EVALUATOR DEPARTMENT: SOS IS

Data Compliance
NIST 800-171: *Strong/Strong*
Maine FOAA: *Strong/Weak (no mention)*
Maine Breach Notification Law: *Weak/Weak (no mention)*
NIST 800-53: Rev5: *Weak/Weak (no mention)*
MaineIT
H1: *Strong/Strong*
H2: *Strong/Adequate*
H3: *Strong/Strong*
A1: *Strong/Adequate*
A2: *Adequate/Adequate (No SDL details, no reference to the environments)*
A3: *Strong/Strong*
A4: *Weak/Weak (no statement or details about copying data free in our format)*
Information Security Standards
S1: *Strong/Strong*
S2: *Strong/Strong*
S3: *Weak/Weak (No 24 hour commitment, otherwise strong)*
S4: *Weak/Weak (no cyber risk appetite statement at link provided)*
S5: *Strong/Strong*
Cloud Service Provider Reqs
CSP1: *Strong/Strong*
CSP2: *Strong/Strong*
CSP3: *Strong/Strong*
CSP4: *Strong/Strong*
CSP5: *Strong/Strong*
CSP6: *Strong/Strong*
CSP7: *Strong/Strong*
CSP8: *Strong/Strong*
CSP9: *Strong/Strong*
CSP10: *Strong/Strong*
CSP11: *Strong/Strong*
CSP12: *Strong/Strong*
CSP13: *Strong/Strong*
CSP14: *Strong/Strong*
NIST Requirement
N1: *Strong/Strong*
N2: *Strong/Strong*
N3: *Strong/Strong*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Microsoft Corporation
DATE: 5-14-24
EVALUATOR NAME: Chris Johnson
EVALUATOR DEPARTMENT: SOS IS

N4: *Strong/Strong*
N5: *Strong/Strong*
N6: *Strong/Strong*
N7: *Strong/Strong (lacking yes/no, but details document yes)*
N8: *Strong/Strong*
N9: *Strong/Strong*
N10: *Strong/Strong*
N11: *Strong/Strong*
N12: *Strong/Strong*
N13: *Strong/Strong*
N14: *Strong/Strong (dashboard showing Azure Environment compliance)*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Microsoft
DATE: 05/13/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

Data Compliance
NIST 800-171: *Quality of Response? strong Quality of Evidence? Adequate*
Maine FOAA: *Quality of Response? Weak Quality of Evidence? weak*
Maine Breach Notification Law: *Quality of Response? Weak Quality of Evidence? weak*
NIST 800-53: Rev5: *Quality of Response? Adequate Quality of Evidence? Adequate*
MaineIT
H1: *Quality of Response? Strong Quality of Evidence? Strong*
H2: *Quality of Response? Adequate Quality of Evidence? Adequate*
H3: *Quality of Response? Adequate Quality of Evidence? weak*
A1: *Quality of Response? Adequate Quality of Evidence? weak*
A2: *Quality of Response? Adequate Quality of Evidence? Adequate*
A3: *Quality of Response? weak Quality of Evidence? weak*
A4: *Quality of Response? Adequate Quality of Evidence? Adequate*
Information Security Standards
S1: *Quality of Response? Adequate Quality of Evidence? Adequate*
S2: *Quality of Response? Adequate Quality of Evidence? Adequate*
S3: *Quality of Response? Adequate Quality of Evidence? Adequate*
S4: *Quality of Response? Strong Quality of Evidence? strong*
S5: *Quality of Response? Adequate Quality of Evidence? weak*
Cloud Service Provider Reqs
CSP1: *Quality of Response? Adequate Quality of Evidence? Adequate*
CSP2: *Quality of Response? Strong Quality of Evidence? Adequate*
CSP3: *Quality of Response? Adequate Quality of Evidence? weak*
CSP4: *Quality of Response? Adequate Quality of Evidence? weak*
CSP5: *Quality of Response? Adequate Quality of Evidence? Adequate*
CSP6: *Quality of Response? Adequate Quality of Evidence? Adequate*
CSP7: *Quality of Response? Strong Quality of Evidence? Adequate*
CSP8: *Quality of Response? Strong Quality of Evidence? Adequate*
CSP9: *Quality of Response? Adequate Quality of Evidence? Adequate*
CSP10: *Quality of Response? Strong Quality of Evidence? Adequate*
CSP11: *Quality of Response? Adequate Quality of Evidence? Adequate*
CSP12: *Quality of Response? Strong Quality of Evidence? Adequate*
CSP13: *Quality of Response? Adequate Quality of Evidence? Adequate*
CSP14: *Quality of Response? Strong Quality of Evidence? Adequate*
NIST Requirement
N1: *Quality of Response? Adequate Quality of Evidence? Adequate*
N2: *Quality of Response? Adequate Quality of Evidence? Adequate*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Microsoft
DATE: 05/13/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

N3: *Quality of Response? Adequate Quality of Evidence? Adequate*
N4: *Quality of Response? Adequate Quality of Evidence? Adequate*
N5: *Quality of Response? Adequate Quality of Evidence? Adequate*
N6: *Quality of Response? Adequate Quality of Evidence? Adequate*
N7: *Quality of Response? Adequate Quality of Evidence? Adequate*
N8: *Quality of Response? Adequate Quality of Evidence? Adequate*
N9: *Quality of Response? Adequate Quality of Evidence? Adequate*
N10: *Quality of Response? Adequate Quality of Evidence? Adequate*
N11: *Quality of Response? Adequate Quality of Evidence? Adequate*
N12: *Quality of Response? Adequate Quality of Evidence? Adequate*
N13: *Quality of Response? Adequate Quality of Evidence? Adequate*
N14: *Quality of Response? Adequate Quality of Evidence? Adequate*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Microsoft
DATE: 10 May 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: DAFS-OIT

Data Compliance
NIST 800-171: *Strong response. Strong evidence..*
Maine FOAA: *Adequate response. Weak (missing) evidence.*
Maine Breach Notification Law: *Adequate response. Weak (missing) evidence.*
NIST 800-53: Rev5: *Strong response. Strong evidence.*
MaineIT
H1: *Strong response. Strong evidence.*
H2: *Strong response. Strong evidence.*
H3: *Strong response. Strong evidence.*
A1: *Adequate response. Adequate evidence.*
A2: *Adequate response. Adequate evidence.*
A3: *Adequate response. Adequate evidence.*
A4: *Adequate response. Adequate evidence.*
Information Security Standards
S1: *Strong response. Strong evidence.*
S2: *Strong response. Strong evidence.*
S3: *Strong response. Strong evidence.*
S4: *Strong response. Strong evidence.*
S5: *Strong response. Strong evidence.*
Cloud Service Provider Reqs
CSP1: *Strong response. Strong evidence.*
CSP2: *Strong response. Strong evidence.*
CSP3: *Strong response. Strong evidence.*
CSP4: *Strong response. Strong evidence.*
CSP5: *Strong response. Strong evidence.*
CSP6: *Strong response. Strong evidence.*
CSP7: *Strong response. Strong evidence.*
CSP8: *Strong response. Strong evidence.*
CSP9: *Strong response. Strong evidence.*
CSP10: *Strong response. Strong evidence.*
CSP11: *Strong response. Strong evidence.*
CSP12: *Strong response. Strong evidence.*
CSP13: *Strong response. Strong evidence.*
CSP14: *Strong response. Strong evidence.*
NIST Requirement
N1: *Strong response. Strong evidence.*
N2: *Strong response. Strong evidence.*
N3: *Strong response. Strong evidence.*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Microsoft
DATE: 10 May 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: DAFS-OIT

N4: *Strong response. Strong evidence.*
N5: *Strong response. Strong evidence.*
N6: *Strong response. Strong evidence.*
N7: *Strong response. Strong evidence.*
N8: *Strong response. Strong evidence.*
N9: *Strong response. Strong evidence.*
N10: *Strong response. Strong evidence.*
N11: *Strong response. Strong evidence.*
N12: *Strong response. Strong evidence.*
N13: *Strong response. Strong evidence.*
N14: *Strong response. Strong evidence.*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: PruTech
DATE: 10 May 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: DAFS-OIT

Data Compliance
NIST 800-171: *Adequate response. Adequate evidence.*
Maine FOAA: *Adequate response. Adequate evidence.*
Maine Breach Notification Law: *Adequate response. Adequate evidence.*
NIST 800-53: Rev5: *Adequate response. Adequate evidence.*
MaineIT
H1: *Adequate response. Weak evidence (Covered Okta, NOT Thales).*
H2: *Adequate response. Adequate evidence.*
H3: *Adequate response. Weak evidence (especially, Thales).*
A1: *Adequate response. Adequate evidence.*
A2: *Adequate response. Adequate evidence.*
A3: *Weak response (“every possible effort”, “times vary”). Adequate evidence.*
A4: *Adequate response. Adequate evidence.*
Information Security Standards
S1: *Adequate response. Adequate evidence.*
S2: *Adequate response. Adequate evidence.*
S3: *Adequate response. Weak evidence (Covered Thales, NOT Okta).*
S4: *Adequate response. Weak evidence (Covered Thales, NOT Okta).*
S5: *Adequate response. Adequate evidence.*
Cloud Service Provider Reqs
CSP1: *Adequate response. Adequate evidence.*
CSP2: *Adequate response. Adequate evidence.*
CSP3: *Adequate response. Adequate evidence.*
CSP4: *Adequate response. Adequate evidence.*
CSP5: *Adequate response. Adequate evidence.*
CSP6: *Adequate response. Adequate evidence.*
CSP7: *Adequate response. Adequate evidence.*
CSP8: *Adequate response. Adequate evidence.*
CSP9: *Adequate response. Adequate evidence.*
CSP10: *Adequate response. Adequate evidence.*
CSP11: *Adequate response. Adequate evidence.*
CSP12: *Adequate response. Adequate evidence.*
CSP13: *Adequate response. Adequate evidence.*
CSP14: *Adequate response. Adequate evidence.*
NIST Requirement
N1: *Adequate response. Adequate evidence.*
N2: *Adequate response. Adequate evidence.*
N3: *Adequate response. Adequate evidence.*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: PruTech
DATE: 10 May 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: DAFS-OIT

N4: *Adequate response. Adequate evidence.*
N5: *Adequate response. Adequate evidence.*
N6: *Adequate response. Adequate evidence.*
N7: *Adequate response. Adequate evidence.*
N8: *Adequate response. Adequate evidence.*
N9: *Adequate response. Adequate evidence.*
N10: *Adequate response. Adequate evidence.*
N11: *Adequate response. Adequate evidence.*
N12: *Adequate response. Adequate evidence.*
N13: *Adequate response. Adequate evidence.*
N14: *NA*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: PruTech Solutions, Inc
DATE: 05/10/2024
EVALUATOR NAME: Ben Haschalk
EVALUATOR DEPARTMENT: DAFS/OIT/ISO

Data Compliance
NIST 800-171: *Quality of Response? Quality of Evidence? Weak / Adequate*
Maine FOAA: *Quality of Response? Quality of Evidence? Weak / Weak*
Maine Breach Notification Law: *Quality of Response? Quality of Evidence? Weak / Weak*
NIST 800-53: Rev5: *Quality of Response? Quality of Evidence? Weak / Adequate*
MaineIT
H1: *Quality of Response? Quality of Evidence? Adequate / Adequate*
H2: *Quality of Response? Quality of Evidence? Adequate / Adequate*
H3: *Quality of Response? Quality of Evidence? Weak / Weak*
A1: *Quality of Response? Quality of Evidence? Adequate / Adequate*
A2: *Quality of Response? Quality of Evidence? Adequate / Adequate*
A3: *Quality of Response? Quality of Evidence? Adequate / Adequate*
A4: *Quality of Response? Quality of Evidence? Adequate / Adequate*
Information Security Standards
S1: *Quality of Response? Quality of Evidence? Adequate / Adequate*
S2: *Quality of Response? Quality of Evidence? Adequate / Adequate*
S3: *Quality of Response? Quality of Evidence? Adequate / Adequate*
S4: *Quality of Response? Quality of Evidence? Adequate / Adequate*
S5: *Quality of Response? Quality of Evidence? Adequate / Adequate*
Cloud Service Provider Reqs
CSP1: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP2: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP3: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP4: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP5: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP6: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP7: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP8: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP9: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP10: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP11: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP12: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP13: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP14: *Quality of Response? Quality of Evidence? Weak / Adequate*
NIST Requirement
N1: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N2: *Quality of Response? Quality of Evidence? Adequate / Adequate*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: PruTech Solutions, Inc
DATE: 05/10/2024
EVALUATOR NAME: Ben Haschalk
EVALUATOR DEPARTMENT: DAFS/OIT/ISO

N3: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N4: *Quality of Response? Quality of Evidence? Weak / Adequate*
N5: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N6: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N7: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N8: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N9: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N10: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N11: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N12: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N13: *Quality of Response? Quality of Evidence? Adequate / Adequate*
N14: *Quality of Response? Quality of Evidence? Adequate / Adequate*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: PruTech Solutions, Inc.
DATE: 5-15-24
EVALUATOR NAME: Chris Johnson
EVALUATOR DEPARTMENT: SOS IS

Data Compliance
NIST 800-171: *Weak/Weak*
Maine FOAA: *Weak/Weak*
Maine Breach Notification Law: *Weak/Weak*
NIST 800-53: Rev5: *Weak/Weak*
MaineIT
H1: *Strong/Strong*
H2: *Weak/Weak (no OneWelcome description or certification of DR, BCP, or backups)*
H3: *Weak/Weak (no OneWelcome practices nor citations)*
A1: *Weak/Weak (no OneWelcome description or certification of DR, BCP, or backups)*
A2: *Weak/Weak (OneWelcome "included")*
A3: *Weak/Weak (Thales only stated uptime in referenced docs and only 99.9 monthly)*
A4: *Weak/Weak (Thales didn't answer data pull or copy free nor ownership)*
Information Security Standards
S1: *Weak/Weak (no NIST claim, no state policy claim, no specifics of SOC2 report type)*
S2: *Weak/Weak*
S3: *Strong/Acceptable*
S4: *Strong/Weak*
S5: *Weak/Weak*
Cloud Service Provider Reqs
CSP1: *Acceptable/Acceptable*
CSP2: *Acceptable/Acceptable*
CSP3: *Strong/Strong*
CSP4: *Weak/Weak (accessibility for Thales not included in references)*
CSP5: *Acceptable/Acceptable*
CSP6: *Acceptable/Acceptable*
CSP7: *Acceptable/Acceptable*
CSP8: *Acceptable/Acceptable*
CSP9: *Acceptable/Acceptable*
CSP10: *Acceptable/Acceptable*
CSP11: *Acceptable/Acceptable*
CSP12: *Acceptable/Acceptable*
CSP13: *Acceptable/Acceptable*
CSP14: *Acceptable/Acceptable*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: PruTech Solutions, Inc.
DATE: 5-15-24
EVALUATOR NAME: Chris Johnson
EVALUATOR DEPARTMENT: SOS IS

NIST Requirement
N1: *Weak/Weak*
N2: *Weak/Weak*
N3: *Weak/Weak*
N4: *Weak/Weak*
N5: *Weak/Weak*
N6: *Weak/Weak*
N7: *Weak/Weak*
N8: *Weak/Weak*
N9: *Weak/Weak*
N10: *Weak/Weak*
N11: *Weak/Weak*
N12: *Weak/Weak*
N13: *Weak/Weak*
N14: *Weak/Weak*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: PruTech
DATE: 5/13/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

Data Compliance
NIST 800-171: *Quality of Response? Weak Quality of Evidence? weak*
Maine FOAA: *Quality of Response? Weak Quality of Evidence? weak*
Maine Breach Notification Law: *Quality of Response? weak Quality of Evidence? weak*
NIST 800-53: Rev5: *Quality of Response? Weak Quality of Evidence? weak*
MaineIT
H1: *Quality of Response? Strong Quality of Evidence? Adequate*
H2: *Quality of Response? Adequate Quality of Evidence? weak*
H3: *Quality of Response? Weak Quality of Evidence? weak*
A1: *Quality of Response? Adequate Quality of Evidence? weak*
A2: *Quality of Response? Adequate Quality of Evidence? weak*
A3: *Quality of Response? Adequate Quality of Evidence? Adequate*
A4: *Quality of Response? Adequate Quality of Evidence? Adequate*
Information Security Standards
S1: *Quality of Response? Weak Quality of Evidence? weak*
S2: *Quality of Response? Weak Quality of Evidence? weak*
S3: *Quality of Response? Weak Quality of Evidence? weak*
S4: *Quality of Response? Weak Quality of Evidence? weak*
S5: *Quality of Response? weak Quality of Evidence? weak*
Cloud Service Provider Reqs
CSP1: *Quality of Response? Weak Quality of Evidence? weak*
CSP2: *Quality of Response? weak Quality of Evidence? weak*
CSP3: *Quality of Response? weak Quality of Evidence? weak*
CSP4: *Quality of Response? weak Quality of Evidence? Weak*
CSP5: *Quality of Response? Weak Quality of Evidence? Weak*
CSP6: *Quality of Response? Weak Quality of Evidence? Weak*
CSP7: *Quality of Response? Weak Quality of Evidence? weak*
CSP8: *Quality of Response? Weak Quality of Evidence? Weak*
CSP9: *Quality of Response? Weak Quality of Evidence? Weak*
CSP10: *Quality of Response? Weak Quality of Evidence? Weak*
CSP11: *Quality of Response? Weak Quality of Evidence? Weak*
CSP12: *Quality of Response? Weak Quality of Evidence? Weak*
CSP13: *Quality of Response? Weak Quality of Evidence? Weak*
CSP14: *Quality of Response? Weak Quality of Evidence? Weak*
NIST Requirement
N1: *Quality of Response? Weak Quality of Evidence? weak*
N2: *Quality of Response? Weak Quality of Evidence? Weak*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: PruTech
DATE: 5/13/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

N3: *Quality of Response? Weak Quality of Evidence? weak*
N4: *Quality of Response? weak Quality of Evidence? weak*
N5: *Quality of Response? Weak Quality of Evidence? weak*
N6: *Quality of Response? weak Quality of Evidence? weak*
N7: *Quality of Response? weak Quality of Evidence? weak*
N8: *Quality of Response? weak Quality of Evidence? weak*
N9: *Quality of Response? weak Quality of Evidence? weak*
N10: *Quality of Response? weak Quality of Evidence? weak*
N11: *Quality of Response? weak Quality of Evidence? weak*
N12: *Quality of Response? weak Quality of Evidence? weak*
N13: *Quality of Response? weak Quality of Evidence? weak*
N14: *Quality of Response? weak Quality of Evidence? weak*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: PruTech
DATE: 5/15/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: Department of Administrative Services

Data Compliance
NIST 800-171: *Quality of Response? Positive Quality of Evidence? Negative*
Maine FOAA: *Quality of Response? Positive Quality of Evidence? Negative*
Maine Breach Notification Law: *Quality of Response? Positive Quality of Evidence? Negative*
NIST 800-53: Rev5: *Quality of Response? Positive Quality of Evidence? Questionable*
MaineIT
H1: *Quality of Response? Positive Quality of Evidence? Positive*
H2: *Quality of Response? Positive Quality of Evidence? Positive*
H3: *Quality of Response? Positive Quality of Evidence? Questionable*
A1: *Quality of Response? Positive Quality of Evidence? Positive*
A2: *Quality of Response? Positive Quality of Evidence? Questionable*
A3: *Quality of Response? Positive Quality of Evidence? Questionable*
A4: *Quality of Response? Positive Quality of Evidence? Questionable*
Information Security Standards
S1: *Quality of Response? Positive Quality of Evidence? Questionable*
S2: *Quality of Response? Positive Quality of Evidence? Positive*
S3: *Quality of Response? Positive Quality of Evidence? Positive*
S4: *Quality of Response? Positive Quality of Evidence? Questionable*
S5: *Quality of Response? Positive Quality of Evidence? Questionable*
Cloud Service Provider Reqs
CSP1: *Quality of Response? Positive Quality of Evidence? Positive*
CSP2: *Quality of Response? Positive Quality of Evidence? Positive*
CSP3: *Quality of Response? Positive Quality of Evidence? Positive*
CSP4: *Quality of Response? Positive Quality of Evidence? Positive*
CSP5: *Quality of Response? Positive Quality of Evidence? Positive*
CSP6: *Quality of Response? Positive Quality of Evidence? Positive*
CSP7: *Quality of Response? Positive Quality of Evidence? Positive*
CSP8: *Quality of Response? Positive Quality of Evidence? Positive*
CSP9: *Quality of Response? Positive Quality of Evidence? Questionable*
CSP10: *Quality of Response? Positive Quality of Evidence? Positive*
CSP11: *Quality of Response? Positive Quality of Evidence? Positive*
CSP12: *Quality of Response? Positive Quality of Evidence? Positive*
CSP13: *Quality of Response? Positive Quality of Evidence? Positive*
CSP14: *Quality of Response? Positive Quality of Evidence? Positive*
NIST Requirement
N1: *Quality of Response? Positive Quality of Evidence? Positive*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: PruTech
DATE: 5/15/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: Department of Administrative Services

N2: *Quality of Response? Positive Quality of Evidence? Positive*
N3: *Quality of Response? Positive Quality of Evidence? Positive*
N4: *Quality of Response? Positive Quality of Evidence? Positive*
N5: *Quality of Response? Positive Quality of Evidence? Positive*
N6: *Quality of Response? Positive Quality of Evidence? Positive*
N7: *Quality of Response? Positive Quality of Evidence? Positive*
N8: *Quality of Response? Positive Quality of Evidence? Positive*
N9: *Quality of Response? Positive Quality of Evidence? Positive*
N10: *Quality of Response? Positive Quality of Evidence? Positive*
N11: *Quality of Response? Positive Quality of Evidence? Positive*
N12: *Quality of Response? Positive Quality of Evidence? Positive*
N13: *Quality of Response? Positive Quality of Evidence? Positive*
N14: *Quality of Response? Positive Quality of Evidence? Positive*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Servos
DATE: 5-15-24
EVALUATOR NAME: Chris Johnson
EVALUATOR DEPARTMENT: SOS IS

Data Compliance
NIST 800-171: *Weak/Weak (27017 not 800-171 equivalence)*
Maine FOAA: *Weak/Weak (not answered)*
Maine Breach Notification Law: *Weak/Weak (not answered)*
NIST 800-53: Rev5: *Acceptable/Acceptable (rough equivalence to ISO27001)*
MaineIT
H1: *Acceptable/Weak (one datacenter plus unspecified GCC)*
H2: *Acceptable/Weak (No reference to Backup+DR plans/process/testing, resting on dual site redundancy)*
H3: *Acceptable/Weak (No reference to problem mgmt, service desk, or citations)*
A1: *Acceptable/Weak (No details)*
A2: *Acceptable/Weak (No details)*
A3: *Strong/Strong*
A4: *Strong/Weak (no reference to pull or copy free)*
Information Security Standards
S1: *Strong/Weak (no claims and artifact is missing)*
S2: *Strong/Strong*
S3: *Strong/Weak (no support for Yes re 24 hours)*
S4: *Acceptable/Weak (unclear re any leadership statement)*
S5: *Acceptable/Weak (by 3rd party - how is that possible if Servos SW?)*
Cloud Service Provider Reqs
CSP1: *Acceptable/Weak (dedicated app or db instance, but not dedicated machines)*
CSP2: *Strong/Weak (artifact not accessible w/o login)*
CSP3: *Strong/Weak (lacks Yes, but good info, artifacts not accessible)*
CSP4: *Strong/Strong (lacks Yes, but good info+artifacts)*
CSP5: *Strong/Weak (lacks Yes, but good info, artifacts not accessible)*
CSP6: *Weak/Weak (lacks Yes, no encryption info, no artifacts)*
CSP7: *Weak/Weak (lacks Yes, info for wrong question)*
CSP8: *Acceptable/Weak (lacks Yes, info but access artifact doesn't exist)*
CSP9: *Acceptable/Strong (lacks Yes, info and artifact OK)*
CSP10: *Acceptable/Strong (lacks Yes, info and artifact OK)*
CSP11: *Acceptable/Strong (lacks Yes, but info OK)*
CSP12: *Weak/Weak (lacks Yes, answer for inc. resp. not sec. assessment..)*
CSP13: *Weak/Weak (lacks Yes, answer misses the mark)*
CSP14: *Weak/Weak (lacks Yes, answer fails to address details or controls)*
NIST Requirement
N1: *Weak/Weak*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Servos
DATE: 5-15-24
EVALUATOR NAME: Chris Johnson
EVALUATOR DEPARTMENT: SOS IS

N2: *Weak/Weak (targets SOM training, not sw or facilities staff)*
N3: *Acceptable/Weak (targets SOM training, not sw or facilities staff)*
N4: *Weak/Weak (end user audit trail, nothing about vendor admins)*
N5: *Weak/Weak (training/awareness oriented, far from complete, no BG Chk)*
N6: *Strong/Strong*
N7: *Acceptable/Weak*
N8: *Acceptable/Acceptable (not clear re identification, but Okta, others are choices)*
N9: *Strong/Weak (nothing re monitoring)*
N10: *Weak/Weak (nothing useful)*
N11: *Strong/Weak (any reports? or audit?)*
N12: *Weak/Weak (nothing about media)*
N13: *Weak/Weak (nothing about supply chain)*
N14: *Acceptable/Weak (certifications available?)*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Servos
DATE: 5/15/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: Department of Administrative Services

Data Compliance
NIST 800-171: *Quality of Response? Positive Quality of Evidence? Questionable*
Maine FOAA: *Quality of Response? Positive Quality of Evidence? Questionable*
Maine Breach Notification Law: *Quality of Response? Positive Quality of Evidence? Questionable*
NIST 800-53: Rev5: *Quality of Response? Positive Quality of Evidence? Questionable*
MaineIT
H1: *Quality of Response? Positive Quality of Evidence? Positive*
H2: *Quality of Response? Positive Quality of Evidence? Positive*
H3: *Quality of Response? Positive Quality of Evidence? Positive*
A1: *Quality of Response? Positive Quality of Evidence? Questionable*
A2: *Quality of Response? Positive Quality of Evidence? Questionable*
A3: *Quality of Response? Positive Quality of Evidence? Questionable*
A4: *Quality of Response? Positive Quality of Evidence? Positive*
Information Security Standards
S1: *Quality of Response? Positive Quality of Evidence? Questionable*
S2: *Quality of Response? Positive Quality of Evidence? Positive*
S3: *Quality of Response? Positive Quality of Evidence? Positive*
S4: *Quality of Response? Positive Quality of Evidence? Positive*
S5: *Quality of Response? Positive Quality of Evidence? Questionable*
Cloud Service Provider Reqs
CSP1: *Quality of Response? Positive Quality of Evidence? Positive*
CSP2: *Quality of Response? Positive Quality of Evidence? Positive*
CSP3: *Quality of Response? Negative Quality of Evidence? Positive*
CSP4: *Quality of Response? Negative Quality of Evidence? Positive*
CSP5: *Quality of Response? Negative Quality of Evidence? Positive*
CSP6: *Quality of Response? Negative Quality of Evidence? Positive*
CSP7: *Quality of Response? Negative Quality of Evidence? Positive*
CSP8: *Quality of Response? Negative Quality of Evidence? Positive*
CSP9: *Quality of Response? Negative Quality of Evidence? Positive*
CSP10: *Quality of Response? Negative Quality of Evidence? Positive*
CSP11: *Quality of Response? Negative Quality of Evidence? Positive*
CSP12: *Quality of Response? Negative Quality of Evidence? Positive*
CSP13: *Quality of Response? Negative Quality of Evidence? Positive*
CSP14: *Quality of Response? Negative Quality of Evidence? Positive*
NIST Requirement
N1: *Quality of Response? Positive Quality of Evidence? Questionable*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Servos
DATE: 5/15/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: Department of Administrative Services

N2: *Quality of Response? Positive Quality of Evidence? Positive*
N3: *Quality of Response? Positive Quality of Evidence? Positive*
N4: *Quality of Response? Positive Quality of Evidence? Positive*
N5: *Quality of Response? Positive Quality of Evidence? Positive*
N6: *Quality of Response? Positive Quality of Evidence? Positive*
N7: *Quality of Response? Positive Quality of Evidence? Positive*
N8: *Quality of Response? Positive Quality of Evidence? Positive*
N9: *Quality of Response? Positive Quality of Evidence? Positive*
N10: *Quality of Response? Positive Quality of Evidence? Positive*
N11: *Quality of Response? Positive Quality of Evidence? Positive*
N12: *Quality of Response? Positive Quality of Evidence? Positive*
N13: *Quality of Response? Positive Quality of Evidence? Positive*
N14: *Quality of Response? Positive Quality of Evidence? Positive*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Servos
DATE: 05/10/2024
EVALUATOR NAME: Ben Haschalk
EVALUATOR DEPARTMENT: DAFS/OIT/ISO

Data Compliance
NIST 800-171: *Quality of Response? Quality of Evidence? Weak / Weak*
Maine FOAA: *Quality of Response? Quality of Evidence? Weak / Weak*
Maine Breach Notification Law: *Quality of Response? Quality of Evidence? Weak / Weak*
NIST 800-53: Rev5: *Quality of Response? Quality of Evidence? Weak / Weak*
MaineIT
H1: *Quality of Response? Quality of Evidence? Weak / Weak*
H2: *Quality of Response? Quality of Evidence? Adequate / Adequate*
H3: *Quality of Response? Quality of Evidence? Adequate / Adequate*
A1: *Quality of Response? Quality of Evidence? Weak / Weak*
A2: *Quality of Response? Quality of Evidence? Weak / Weak*
A3: *Quality of Response? Quality of Evidence? Adequate / Adequate*
A4: *Quality of Response? Quality of Evidence? Adequate / Adequate*
Information Security Standards
S1: *Quality of Response? Quality of Evidence? Weak / Adequate*
S2: *Quality of Response? Quality of Evidence? Adequate / Adequate*
S3: *Quality of Response? Quality of Evidence? Adequate / Adequate*
S4: *Quality of Response? Quality of Evidence? Adequate / Adequate*
S5: *Quality of Response? Quality of Evidence? Adequate / Adequate*
Cloud Service Provider Reqs
CSP1: *Quality of Response? Quality of Evidence? Weak / Adequate*
CSP2: *Quality of Response? Quality of Evidence? Weak / Adequate*
CSP3: *Quality of Response? Quality of Evidence? Weak / Adequate*
CSP4: *Quality of Response? Quality of Evidence? Weak / Weak*
CSP5: *Quality of Response? Quality of Evidence? Weak / Adequate*
CSP6: *Quality of Response? Quality of Evidence? Weak / Adequate*
CSP7: *Quality of Response? Quality of Evidence? Weak / Adequate*
CSP8: *Quality of Response? Quality of Evidence? Weak / Adequate*
CSP9: *Quality of Response? Quality of Evidence? Weak / Adequate*
CSP10: *Quality of Response? Quality of Evidence? Weak / Adequate*
CSP11: *Quality of Response? Quality of Evidence? Weak / Adequate*
CSP12: *Quality of Response? Quality of Evidence? Weak / Adequate*
CSP13: *Quality of Response? Quality of Evidence? Weak / Adequate*
CSP14: *Quality of Response? Quality of Evidence? Weak / Adequate*
NIST Requirement
N1: *Quality of Response? Quality of Evidence? Weak / Adequate*
N2: *Quality of Response? Quality of Evidence? Weak / Adequate*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Servos
DATE: 05/10/2024
EVALUATOR NAME: Ben Haschalk
EVALUATOR DEPARTMENT: DAFS/OIT/ISO

N3: *Quality of Response? Quality of Evidence? Weak / Adequate*
N4: *Quality of Response? Quality of Evidence? Weak / Adequate*
N5: *Quality of Response? Quality of Evidence? Weak / Adequate*
N6: *Quality of Response? Quality of Evidence? Weak / Adequate*
N7: *Quality of Response? Quality of Evidence? Weak / Adequate*
N8: *Quality of Response? Quality of Evidence? Weak / Adequate*
N9: *Quality of Response? Quality of Evidence? Weak / Adequate*
N10: *Quality of Response? Quality of Evidence? Weak / Weak*
N11: *Quality of Response? Quality of Evidence? Weak / Adequate*
N12: *Quality of Response? Quality of Evidence? Weak / Weak*
N13: *Quality of Response? Quality of Evidence? Weak / Adequate*
N14: *Quality of Response? Quality of Evidence? Weak / Adequate*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Servos
DATE: 5/15/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

Data Compliance
NIST 800-171: *Quality of Response? Adequate Quality of Evidence? weak*
Maine FOAA: *Quality of Response? Adequate Quality of Evidence? weak*
Maine Breach Notification Law: *Quality of Response? Adequate Quality of Evidence? weak*
NIST 800-53: Rev5: *Quality of Response? Adequate Quality of Evidence? weak*
MaineIT
H1: *Quality of Response? Adequate Quality of Evidence? Adequate*
H2: *Quality of Response? Adequate Quality of Evidence? Adequate*
H3: *Quality of Response? Adequate Quality of Evidence? Weak*
A1: *Quality of Response? weak Quality of Evidence? weak*
A2: *Quality of Response? Weak Quality of Evidence? weak*
A3: *Quality of Response? Adequate Quality of Evidence? weak*
A4: *Quality of Response? Adequate Quality of Evidence? weak*
Information Security Standards
S1: *Quality of Response? Weak Quality of Evidence? weak*
S2: *Quality of Response? Adequate Quality of Evidence? Adequate*
S3: *Quality of Response? Adequate Quality of Evidence? weak*
S4: *Quality of Response? Adequate Quality of Evidence? weak*
S5: *Quality of Response? Adequate Quality of Evidence? weak*
Cloud Service Provider Reqs
CSP1: *Quality of Response? Adequate Quality of Evidence? weak*
CSP2: *Quality of Response? Adequate Quality of Evidence? weak*
CSP3: *Quality of Response? weak Quality of Evidence? weak*
CSP4: *Quality of Response? Adequate Quality of Evidence? weak*
CSP5: *Quality of Response? Adequate Quality of Evidence? Weak*
CSP6: *Quality of Response? Adequate Quality of Evidence? Weak*
CSP7: *Quality of Response? Adequate Quality of Evidence? Weak*
CSP8: *Quality of Response? Adequate Quality of Evidence? Weak*
CSP9: *Quality of Response? Adequate Quality of Evidence? Weak*
CSP10: *Quality of Response? Adequate Quality of Evidence? Weak*
CSP11: *Quality of Response? Adequate Quality of Evidence? Weak*
CSP12: *Quality of Response? Adequate Quality of Evidence? Weak*
CSP13: *Quality of Response? Adequate Quality of Evidence? Weak*
CSP14: *Quality of Response? Adequate Quality of Evidence? weak*
NIST Requirement
N1: *Quality of Response? weak Quality of Evidence? weak*
N2: *Quality of Response? Weak Quality of Evidence? weak*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Servos
DATE: 5/15/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

N3: *Quality of Response? weak Quality of Evidence? weak*
N4: *Quality of Response? weak Quality of Evidence? weak*
N5: *Quality of Response? weak Quality of Evidence? weak*
N6: *Quality of Response? weak Quality of Evidence? weak*
N7: *Quality of Response? weak Quality of Evidence? weak*
N8: *Quality of Response? weak Quality of Evidence? weak*
N9: *Quality of Response? weak Quality of Evidence? weak*
N10: *Quality of Response? weak Quality of Evidence? weak*
N11: *Quality of Response? weak Quality of Evidence? weak*
N12: *Quality of Response? weak Quality of Evidence? weak*
N13: *Quality of Response? weak Quality of Evidence? weak*
N14: *Quality of Response? weak Quality of Evidence? weak*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Servos
DATE: 10 May 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: DAFS-OIT

Data Compliance
NIST 800-171: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
Maine FOAA: *Adequate response. Weak (missing) evidence.*
Maine Breach Notification Law: *Adequate response. Weak (missing) evidence.*
NIST 800-53: Rev5: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
MaineIT
H1: *Adequate response. Weak evidence (No specific details).*
H2: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
H3: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
A1: *Adequate response. Weak evidence (No specific details).*
A2: *Adequate response. Weak evidence (No specific details).*
A3: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
A4: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
Information Security Standards
S1: *Adequate response. Weak evidence (Missing “Data Security Addendum”).*
S2: *Adequate response. Adequate evidence.*
S3: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
S4: *Adequate response. Weak evidence (No specific details).*
S5: *Adequate response. Weak evidence (No specific details).*
Cloud Service Provider Reqs
CSP1: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
CSP2: *Adequate response.. Weak evidence (Covered ServiceNow, NOT ID.me).*
CSP3: *Weak response (Blank). Weak evidence (Covered ServiceNow, NOT ID.me).*
CSP4: *Weak response (Blank). Weak evidence (Covered ServiceNow, NOT ID.me).*
CSP5: *Weak response (Blank). Weak evidence (Covered ServiceNow, NOT ID.me).*
CSP6: *Weak response (Blank). Weak evidence (Covered ServiceNow, NOT ID.me).*
CSP7: *Weak response (Blank). Weak evidence (Covered ServiceNow, NOT ID.me).*
CSP8: *Weak response (Blank). Weak evidence (Covered ServiceNow, NOT ID.me).*
CSP9: *Weak response (Blank). Weak evidence (Covered ServiceNow, NOT ID.me).*
CSP10: *Weak response (Blank). Weak evidence (Covered ServiceNow, NOT ID.me).*
CSP11: *Weak response (Blank). Weak evidence (Covered ServiceNow, NOT ID.me).*
CSP12: *Weak response (Blank). Weak evidence (Covered ServiceNow, NOT ID.me).*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Servos
DATE: 10 May 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: DAFS-OIT

CSP13: *Weak response (Blank). Weak evidence (Covered ServiceNow, NOT ID.me).*
CSP14: *Weak response (Blank). Weak evidence (Covered ServiceNow, NOT ID.me).*
NIST Requirement
N1: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
N2: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
N3: *Adequate response. Weak evidence (No specific details).*
N4: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
N5: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
N6: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
N7: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
N8: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
N9: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
N10: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
N11: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
N12: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
N13: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*
N14: *Adequate response. Weak evidence (Covered ServiceNow, NOT ID.me).*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Tyler
DATE: 5/15/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: Department of Administrative Services

Data Compliance
NIST 800-171: *Quality of Response? Positive Quality of Evidence? Positive*
Maine FOAA: *Quality of Response? Positive Quality of Evidence? Positive*
Maine Breach Notification Law: *Quality of Response? Positive Quality of Evidence? Positive*
NIST 800-53: Rev5: *Quality of Response? Positive Quality of Evidence? Positive*
MaineIT
H1: *Quality of Response? Positive Quality of Evidence? Positive*
H2: *Quality of Response? Positive Quality of Evidence? Positive*
H3: *Quality of Response? Positive Quality of Evidence? Positive*
A1: *Quality of Response? Positive Quality of Evidence? Positive*
A2: *Quality of Response? Positive Quality of Evidence? Positive*
A3: *Quality of Response? Positive Quality of Evidence? Positive*
A4: *Quality of Response? Positive Quality of Evidence? Positive*
Information Security Standards
S1: *Quality of Response? Positive Quality of Evidence? Positive*
S2: *Quality of Response? Positive Quality of Evidence? Positive*
S3: *Quality of Response? Positive Quality of Evidence? Positive*
S4: *Quality of Response? Negative Quality of Evidence? Positive*
S5: *Quality of Response? Negative Quality of Evidence? Positive*
Cloud Service Provider Reqs
CSP1: *Quality of Response? Positive Quality of Evidence? Positive*
CSP2: *Quality of Response? Positive Quality of Evidence? Positive*
CSP3: *Quality of Response? Positive Quality of Evidence? Positive*
CSP4: *Quality of Response? Positive Quality of Evidence? Positive*
CSP5: *Quality of Response? Positive Quality of Evidence? Positive*
CSP6: *Quality of Response? Positive Quality of Evidence? Positive*
CSP7: *Quality of Response? Positive Quality of Evidence? Positive*
CSP8: *Quality of Response? Positive Quality of Evidence? Positive*
CSP9: *Quality of Response? Positive Quality of Evidence? Positive*
CSP10: *Quality of Response? Positive Quality of Evidence? Positive*
CSP11: *Quality of Response? Positive Quality of Evidence? Positive*
CSP12: *Quality of Response? Positive Quality of Evidence? Positive*
CSP13: *Quality of Response? Positive Quality of Evidence? Positive*
CSP14: *Quality of Response? Positive Quality of Evidence? Positive*
NIST Requirement
N1: *Quality of Response? Positive Quality of Evidence? Positive*
N2: *Quality of Response? Positive Quality of Evidence? Positive*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Tyler
DATE: 5/15/24
EVALUATOR NAME: Craig Locke
EVALUATOR DEPARTMENT: Department of Administrative Services

N3: *Quality of Response? Positive Quality of Evidence? Positive*
N4: *Quality of Response? Positive Quality of Evidence? Positive*
N5: *Quality of Response? Positive Quality of Evidence? Positive*
N6: *Quality of Response? Positive Quality of Evidence? Positive*
N7: *Quality of Response? Positive Quality of Evidence? Positive*
N8: *Quality of Response? Positive Quality of Evidence? Positive*
N9: *Quality of Response? Positive Quality of Evidence? Positive*
N10: *Quality of Response? Positive Quality of Evidence? Positive*
N11: *Quality of Response? Positive Quality of Evidence? Positive*
N12: *Quality of Response? Positive Quality of Evidence? Positive*
N13: *Quality of Response? Positive Quality of Evidence? Positive*
N14: *Quality of Response? Positive Quality of Evidence? Positive*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Tyler Maine
DATE: 05/10/2024
EVALUATOR NAME: Ben Haschalk
EVALUATOR DEPARTMENT: DAFS/OIT/ISO

Data Compliance
NIST 800-171: *Quality of Response? Quality of Evidence? Adequate / Adequate*
Maine FOAA: *Quality of Response? Quality of Evidence? Adequate / Adequate*
Maine Breach Notification Law: *Quality of Response? Quality of Evidence? Adequate / Adequate*
NIST 800-53: Rev5: *Quality of Response? Quality of Evidence? Adequate / Adequate*
MaineIT
H1: *Quality of Response? Quality of Evidence? Adequate / Adequate*
H2: *Quality of Response? Quality of Evidence? Adequate / Adequate*
H3: *Quality of Response? Quality of Evidence? Adequate / Adequate*
A1: *Quality of Response? Quality of Evidence? Adequate / Adequate*
A2: *Quality of Response? Quality of Evidence? Adequate / Adequate*
A3: *Quality of Response? Quality of Evidence? Adequate / Adequate*
A4: *Quality of Response? Quality of Evidence? Adequate / Adequate*
Information Security Standards
S1: *Quality of Response? Quality of Evidence? Adequate / Adequate*
S2: *Quality of Response? Quality of Evidence? Adequate / Adequate*
S3: *Quality of Response? Quality of Evidence? Adequate / Adequate*
S4: *Quality of Response? Quality of Evidence? Adequate / Adequate*
S5: *Quality of Response? Quality of Evidence? Adequate / Adequate*
Cloud Service Provider Reqs
CSP1: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP2: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP3: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP4: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP5: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP6: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP7: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP8: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP9: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP10: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP11: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP12: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP13: *Quality of Response? Quality of Evidence? Adequate / Adequate*
CSP14: *Quality of Response? Quality of Evidence? Adequate / Adequate*
NIST Requirement
N1: *Quality of Response? Quality of Evidence? Weak / Adequate*
N2: *Quality of Response? Quality of Evidence? Weak / Adequate*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Tyler Maine
DATE: 05/10/2024
EVALUATOR NAME: Ben Haschalk
EVALUATOR DEPARTMENT: DAFS/OIT/ISO

N3: *Quality of Response? Quality of Evidence? Weak / Adequate*
N4: *Quality of Response? Quality of Evidence? Weak / Adequate*
N5: *Quality of Response? Quality of Evidence? Weak / Adequate*
N6: *Quality of Response? Quality of Evidence? Weak / Adequate*
N7: *Quality of Response? Quality of Evidence? Weak / Adequate*
N8: *Quality of Response? Quality of Evidence? Weak / Adequate*
N9: *Quality of Response? Quality of Evidence? Weak / Adequate*
N10: *Quality of Response? Quality of Evidence? Weak / Adequate*
N11: *Quality of Response? Quality of Evidence? Weak / Adequate*
N12: *Quality of Response? Quality of Evidence? Weak / Adequate*
N13: *Quality of Response? Quality of Evidence? Weak / Adequate*
N14: *Quality of Response? Quality of Evidence? Adequate / Adequate*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Tyler Maine
DATE: 5-15-24
EVALUATOR NAME: Chris Johnson
EVALUATOR DEPARTMENT: SOS IS

Data Compliance
NIST 800-171: *Strong/Strong*
Maine FOAA: *Strong/Strong*
Maine Breach Notification Law: *Strong/Strong*
NIST 800-53: Rev5: *Strong/Strong*
MaineIT
H1: *Strong/Strong*
H2: *Strong/Strong*
H3: *Strong/Strong*
A1: *Strong/Strong*
A2: *Strong/Strong*
A3: *Strong/Weak*
A4: *Strong/Strong*
Information Security Standards
S1: *Strong/Strong*
S2: *Strong/Strong*
S3: *Strong/Acceptable*
S4: *Weak/Acceptable (These were conditional, so does this constitute N/A?)*
S5: *Weak/Weak (These were conditional, so does this constitute N/A?)*
Cloud Service Provider Reqs
CSP1: *Strong/Acceptable*
CSP2: *Strong/Strong*
CSP3: *Strong/Strong*
CSP4: *Strong/Strong*
CSP5: *Strong/Strong*
CSP6: *Strong/Strong*
CSP7: *Strong/Strong*
CSP8: *Strong/Strong*
CSP9: *Strong/Strong*
CSP10: *Strong/Strong*
CSP11: *Strong/Strong*
CSP12: *Strong/Strong*
CSP13: *Strong/Strong*
CSP14: *Strong/Strong*
NIST Requirement
N1: *Strong/Strong*
N2: *Strong/Strong*
N3: *Strong/Strong*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Tyler Maine
DATE: 5-15-24
EVALUATOR NAME: Chris Johnson
EVALUATOR DEPARTMENT: SOS IS

N4: *Strong/Strong*
N5: *Strong/Strong*
N6: *Strong/Strong*
N7: *Strong/Strong*
N8: *Strong/Strong*
N9: *Strong/Strong*
N10: *Strong/Strong*
N11: *Strong/Strong*
N12: *Strong/Strong*
N13: *Strong/Strong*
N14: *Strong/Strong*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Tyler
DATE: 05/15/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

Data Compliance
NIST 800-171: *Quality of Response? Strong Quality of Evidence? Adequate*
Maine FOAA: *Quality of Response? Adequate Quality of Evidence? Adequate*
Maine Breach Notification Law: *Quality of Response? Adequate Quality of Evidence? Adequate*
NIST 800-53: Rev5: *Quality of Response? Strong Quality of Evidence? Strong*
MaineIT
H1: *Quality of Response? Adequate Quality of Evidence? Adequate*
H2: *Quality of Response? Adequate Quality of Evidence? Adequate*
H3: *Quality of Response? Adequate Quality of Evidence? Adequate*
A1: *Quality of Response? Adequate Quality of Evidence? strong*
A2: *Quality of Response? Strong Quality of Evidence? Strong*
A3: *Quality of Response? Strong Quality of Evidence? Strong*
A4: *Quality of Response? Adequate Quality of Evidence? Adequate*
Information Security Standards
S1: *Quality of Response? Adequate Quality of Evidence? Adequate*
S2: *Quality of Response? Adequate Quality of Evidence? Adequate*
S3: *Quality of Response? Adequate Quality of Evidence? Adequate*
S4: *Quality of Response? Adequate Quality of Evidence? Adequate*
S5: *Quality of Response? Adequate Quality of Evidence? Adequate*
Cloud Service Provider Reqs
CSP1: *Quality of Response? Adequate Quality of Evidence? Adequate*
CSP2: *Quality of Response? Adequate Quality of Evidence? Adequate*
CSP3: *Quality of Response? Adequate Quality of Evidence? Adequate*
CSP4: *Quality of Response? Adequate Quality of Evidence? Adequate*
CSP5: *Quality of Response? Adequate Quality of Evidence? Adequate*
CSP6: *Quality of Response? Adequate Quality of Evidence? Adequate*
CSP7: *Quality of Response? Adequate Quality of Evidence? Adequate*
CSP8: *Quality of Response? Adequate Quality of Evidence? Adequate*
CSP9: *Quality of Response? Adequate Quality of Evidence? Adequate*
CSP10: *Quality of Response? Adequate Quality of Evidence? Adequate*
CSP11: *Quality of Response? Adequate Quality of Evidence? Adequate*
CSP12: *Quality of Response? Adequate Quality of Evidence? Adequate*
CSP13: *Quality of Response? Adequate Quality of Evidence? Adequate*
CSP14: *Quality of Response? Adequate Quality of Evidence? Adequate*
NIST Requirement
N1: *Quality of Response? Adequate Quality of Evidence? Adequate*
N2: *Quality of Response? Adequate Quality of Evidence? Adequate*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Tyler
DATE: 05/15/2024
EVALUATOR NAME: Dave Pascarella
EVALUATOR DEPARTMENT: MaineIT

N3: *Quality of Response? Adequate Quality of Evidence? Adequate*
N4: *Quality of Response? Adequate Quality of Evidence? Adequate*
N5: *Quality of Response? Adequate Quality of Evidence? Adequate*
N6: *Quality of Response? Adequate Quality of Evidence? Adequate*
N7: *Quality of Response? Adequate Quality of Evidence? Adequate*
N8: *Quality of Response? Adequate Quality of Evidence? Adequate*
N9: *Quality of Response? Adequate Quality of Evidence? Adequate*
N10: *Quality of Response? Adequate Quality of Evidence? Adequate*
N11: *Quality of Response? Adequate Quality of Evidence? Adequate*
N12: *Quality of Response? Adequate Quality of Evidence? Adequate*
N13: *Quality of Response? Adequate Quality of Evidence? Adequate*
N14: *Quality of Response? Adequate Quality of Evidence? Adequate*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Tyler
DATE: 06 May 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: DAFS-OIT

Data Compliance
NIST 800-171: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
Maine FOAA: *Adequate response. Adequate evidence.*
Maine Breach Notification Law: *Adequate response. Adequate evidence.*
NIST 800-53: Rev5: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
MaineIT
H1: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
H2: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
H3: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
A1: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
A2: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
A3: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
A4: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
Information Security Standards
S1: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
S2: *Adequate response. Adequate evidence.*
S3: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
S4: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
S5: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
Cloud Service Provider Reqs
CSP1: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
CSP2: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Tyler
DATE: 06 May 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: DAFS-OIT

CSP3: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
CSP4: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
CSP5: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
CSP6: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
CSP7: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
CSP8: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
CSP9: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
CSP10: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
CSP11: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
CSP12: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
CSP13: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
CSP14: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
NIST Requirement
N1: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
N2: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
N3: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
N4: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
N5: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
N6: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*

STATE OF MAINE
INDIVIDUAL EVALUATION NOTES - TECHNICAL ASSESSMENT

RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents
BIDDER NAME: Tyler
DATE: 06 May 2024
EVALUATOR NAME: B. Victor Chakravarty
EVALUATOR DEPARTMENT: DAFS-OIT

N7: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
N8: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
N9: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
N10: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
N11: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
N12: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
N13: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*
N14: *Adequate response. Weak evidence (Covered Tyler, NOT Okta, NOT Socure ID+).*

STATE OF MAINE
DEPARTMENT OF ADMINISTRATIVE
AND FINANCIAL SERVICES - MaineIT

Janet T. Mills
Governor

Kirsten Figueroa
Commissioner

AGREEMENT AND DISCLOSURE STATEMENT
RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents

I, Ben Haschalk, accept the offer to become a member of the Request for Proposals (RFP) Evaluation Team for the State of Maine Department of Administrative and Financial Services, MaineIT. I do hereby accept the terms set forth in this agreement AND hereby disclose any affiliation or relationship I may have in connection with a bidder who has submitted a proposal to this RFP.

Neither I nor any member of my immediate family have a personal or financial interest, direct or indirect, in the bidders whose proposals I will be reviewing. “Interest” may include, but is not limited to: current or former ownership in the bidder’s company; current or former Board membership; current or former employment with the bidder; current or former personal contractual relationship with the bidder (example: paid consultant); and/or current or former relationship to a bidder’s official which could reasonably be construed to constitute a conflict of interest (personal relationships may be perceived by the public as a potential conflict of interest).

I have not advised, consulted with or assisted any bidder in the preparation of any proposal submitted in response to this RFP nor have I submitted a letter of support or similar endorsement.

I understand and agree that the evaluation process is to be conducted in an impartial manner without bias or prejudice. In this regard, I hereby certify that, to the best of my knowledge, there are no circumstances that would reasonably support a good faith charge of bias. I further understand that in the event a good faith charge of bias is made, it will rest with me to decide whether I should be disqualified from participation in the evaluation process.

I agree to hold confidential all information related to the contents of Requests for Proposals presented during the review process until such time as the Department formally releases the award decision notices for public distribution.

Ben Haschalk

Signature

04/19/2024

Date

STATE OF MAINE
DEPARTMENT OF ADMINISTRATIVE AND FINANCIAL SERVICES - MaineIT

Janet T. Mills
Governor

Kirsten Figueroa
Commissioner

AGREEMENT AND DISCLOSURE STATEMENT
RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents

I, Chris Johnson, accept the offer to become a member of the Request for Proposals (RFP) Evaluation Team for the State of Maine Department of Administrative and Financial Services, MaineIT. I do hereby accept the terms set forth in this agreement AND hereby disclose any affiliation or relationship I may have in connection with a bidder who has submitted a proposal to this RFP.

Neither I nor any member of my immediate family have a personal or financial interest, direct or indirect, in the bidders whose proposals I will be reviewing. “Interest” may include, but is not limited to: current or former ownership in the bidder’s company; current or former Board membership; current or former employment with the bidder; current or former personal contractual relationship with the bidder (example: paid consultant); and/or current or former relationship to a bidder’s official which could reasonably be construed to constitute a conflict of interest (personal relationships may be perceived by the public as a potential conflict of interest).

I have not advised, consulted with or assisted any bidder in the preparation of any proposal submitted in response to this RFP nor have I submitted a letter of support or similar endorsement.

I understand and agree that the evaluation process is to be conducted in an impartial manner without bias or prejudice. In this regard, I hereby certify that, to the best of my knowledge, there are no circumstances that would reasonably support a good faith charge of bias. I further understand that in the event a good faith charge of bias is made, it will rest with me to decide whether I should be disqualified from participation in the evaluation process.

I agree to hold confidential all information related to the contents of Requests for Proposals presented during the review process until such time as the Department formally releases the award decision notices for public distribution.

Christopher N. Johnson
Signature

4-22-2024
Date

STATE OF MAINE
DEPARTMENT OF ADMINISTRATIVE
AND FINANCIAL SERVICES - MaineIT

Janet T. Mills
Governor

Kirsten Figueroa
Commissioner

AGREEMENT AND DISCLOSURE STATEMENT
RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents

I, Craig Locke, accept the offer to become a member of the Request for Proposals (RFP) Evaluation Team for the State of Maine Department of Administrative and Financial Services, MaineIT. I do hereby accept the terms set forth in this agreement AND hereby disclose any affiliation or relationship I may have in connection with a bidder who has submitted a proposal to this RFP.

Neither I nor any member of my immediate family have a personal or financial interest, direct or indirect, in the bidders whose proposals I will be reviewing. "Interest" may include, but is not limited to: current or former ownership in the bidder's company; current or former Board membership; current or former employment with the bidder; current or former personal contractual relationship with the bidder (example: paid consultant); and/or current or former relationship to a bidder's official which could reasonably be construed to constitute a conflict of interest (personal relationships may be perceived by the public as a potential conflict of interest).

I have not advised, consulted with or assisted any bidder in the preparation of any proposal submitted in response to this RFP nor have I submitted a letter of support or similar endorsement.

I understand and agree that the evaluation process is to be conducted in an impartial manner without bias or prejudice. In this regard, I hereby certify that, to the best of my knowledge, there are no circumstances that would reasonably support a good faith charge of bias. I further understand that in the event a good faith charge of bias is made, it will rest with me to decide whether I should be disqualified from participation in the evaluation process.

I agree to hold confidential all information related to the contents of Requests for Proposals presented during the review process until such time as the Department formally releases the award decision notices for public distribution.

Craig Locke
Signature

4/22/24
Date

STATE OF MAINE
DEPARTMENT OF ADMINISTRATIVE AND FINANCIAL SERVICES - MaineIT

Janet T. Mills
Governor

Kirsten Figueroa
Commissioner

AGREEMENT AND DISCLOSURE STATEMENT
RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents

I, Dave Pascarella accept the offer to become a member of the Request for Proposals (RFP) Evaluation Team for the State of Maine Department of Administrative and Financial Services, MaineIT. I do hereby accept the terms set forth in this agreement AND hereby disclose any affiliation or relationship I may have in connection with a bidder who has submitted a proposal to this RFP.

Neither I nor any member of my immediate family have a personal or financial interest, direct or indirect, in the bidders whose proposals I will be reviewing. “Interest” may include, but is not limited to: current or former ownership in the bidder’s company; current or former Board membership; current or former employment with the bidder; current or former personal contractual relationship with the bidder (example: paid consultant); and/or current or former relationship to a bidder’s official which could reasonably be construed to constitute a conflict of interest (personal relationships may be perceived by the public as a potential conflict of interest).

I have not advised, consulted with or assisted any bidder in the preparation of any proposal submitted in response to this RFP nor have I submitted a letter of support or similar endorsement.

I understand and agree that the evaluation process is to be conducted in an impartial manner without bias or prejudice. In this regard, I hereby certify that, to the best of my knowledge, there are no circumstances that would reasonably support a good faith charge of bias. I further understand that in the event a good faith charge of bias is made, it will rest with me to decide whether I should be disqualified from participation in the evaluation process.

I agree to hold confidential all information related to the contents of Requests for Proposals presented during the review process until such time as the Department formally releases the award decision notices for public distribution.

David Pascarella
Signature

4/22/2024
Date

STATE OF MAINE
DEPARTMENT OF ADMINISTRATIVE
AND FINANCIAL SERVICES - MaineIT

Janet T. Mills
Governor

Kirsten Figueroa
Commissioner

AGREEMENT AND DISCLOSURE STATEMENT
RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents

I, Lisa Leahy, accept the offer to become a member of the Request for Proposals (RFP) Evaluation Team for the State of Maine Department of Administrative and Financial Services, MaineIT. I do hereby accept the terms set forth in this agreement AND hereby disclose any affiliation or relationship I may have in connection with a bidder who has submitted a proposal to this RFP.

Neither I nor any member of my immediate family have a personal or financial interest, direct or indirect, in the bidders whose proposals I will be reviewing. “Interest” may include, but is not limited to: current or former ownership in the bidder’s company; current or former Board membership; current or former employment with the bidder; current or former personal contractual relationship with the bidder (example: paid consultant); and/or current or former relationship to a bidder’s official which could reasonably be construed to constitute a conflict of interest (personal relationships may be perceived by the public as a potential conflict of interest).

I have not advised, consulted with or assisted any bidder in the preparation of any proposal submitted in response to this RFP nor have I submitted a letter of support or similar endorsement.

I understand and agree that the evaluation process is to be conducted in an impartial manner without bias or prejudice. In this regard, I hereby certify that, to the best of my knowledge, there are no circumstances that would reasonably support a good faith charge of bias. I further understand that in the event a good faith charge of bias is made, it will rest with me to decide whether I should be disqualified from participation in the evaluation process.

I agree to hold confidential all information related to the contents of Requests for Proposals presented during the review process until such time as the Department formally releases the award decision notices for public distribution.

Lisa Leahy	**4/19/24**
Signature	**Date**

STATE OF MAINE
DEPARTMENT OF ADMINISTRATIVE
AND FINANCIAL SERVICES - MaineIT

Janet T. Mills
Governor

Kirsten Figueroa
Commissioner

AGREEMENT AND DISCLOSURE STATEMENT
RFP #: 202401005
RFP TITLE: Improve Delivery of Digital Services to Constituents

I, Victor Chakravarty, accept the offer to become a member of the Request for Proposals (RFP) Evaluation Team for the State of Maine Department of Administrative and Financial Services, MaineIT. I do hereby accept the terms set forth in this agreement AND hereby disclose any affiliation or relationship I may have in connection with a bidder who has submitted a proposal to this RFP.

Neither I nor any member of my immediate family have a personal or financial interest, direct or indirect, in the bidders whose proposals I will be reviewing. “Interest” may include, but is not limited to: current or former ownership in the bidder’s company; current or former Board membership; current or former employment with the bidder; current or former personal contractual relationship with the bidder (example: paid consultant); and/or current or former relationship to a bidder’s official which could reasonably be construed to constitute a conflict of interest (personal relationships may be perceived by the public as a potential conflict of interest).

I have not advised, consulted with or assisted any bidder in the preparation of any proposal submitted in response to this RFP nor have I submitted a letter of support or similar endorsement.

I understand and agree that the evaluation process is to be conducted in an impartial manner without bias or prejudice. In this regard, I hereby certify that, to the best of my knowledge, there are no circumstances that would reasonably support a good faith charge of bias. I further understand that in the event a good faith charge of bias is made, it will rest with me to decide whether I should be disqualified from participation in the evaluation process.

I agree to hold confidential all information related to the contents of Requests for Proposals presented during the review process until such time as the Department formally releases the award decision notices for public distribution.

B. Victor Chakravarty

18 April 2024

Signature **Date**