State of Maine
Department of Administrative and Financial Services
Office of Information Technology

Security Assessment and Authorization Policy and Procedures (CA-1)

Table of Contents

1.0. Document Purpose

The purpose of this document is to define the State of Maine policy and procedures the Office of Information Technology (OIT) uses to conduct and support security assessments of information assets (see Definitions) and to determine whether they meet specific security objectives. This document corresponds to the Security Assessment and Authorization Control Family of National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 4).

2.0. Scope

2.1. This policy applies to all State of Maine employees and contractors (collectively referred to as personnel in this document) with access to:

- 2.1.1. Executive Branch Agency information assets, irrespective of location; and
- 2.1.2. Information assets from other State government branches that use Executive Branch managed services.

3.0. Policy Conflict

If this policy conflicts with any law or union contract in effect, the terms of the existing law or contract prevail.

4.0. Roles and Responsibilities

4.1. Agencies

- 4.1.1. Ensure that contracts for vendor-hosted or -managed agency information systems adhere to pertinent Federal regulations, State regulations, and OIT policies, procedures, and standards.
- 4.1.2. Ensure agency personnel are aware of applicable penalties for compliance violations.
- 4.1.3. Develop and implement agency-level policy and procedures to meet additional security assessment and authorization regulatory requirements.
- 4.1.4. Directly coordinate to meet compliance requirements for State and Federal audit documentation, reporting, and onsite logistic support.

4.2. IT Procurement

- 4.2.1. Collaborates with OIT Information Asset Owners and agencies to ensure vendor contracts contain appropriate security requirement language.

4.3. OIT Information Asset Owners

- 4.3.1. Collaborate with IT Procurement and agency business partners to ensure interconnections with vendors are properly documented.

4.4. Information Security Office Responsibilities

- 4.4.1. Conduct assessments to identify exploitable weaknesses in information technology systems.
- 4.4.2. Use assessment results to improve OIT's proactive information security defense.
- 4.4.3. Remediate known, systemic information security audit findings, and develop systems to improve State of Maine information security inspection results.

4.4.4. Assist State of Maine agencies in improving the security for numerous data types including, but not limited to, Federal Tax Information (FTI) (see Definitions), Social Security, Affordable Care Act, criminal justice, credit card, health, and Personally Identifiable Information.

4.4.5. Provide information technology responses and assist with remediating security audits conducted by the Internal Revenue Service (IRS), the Centers for Medicare & Medicaid Services (CMS), the Federal Bureau of Investigation (FBI), the U.S. Department of Health and Human Services (U.S. DHHS), the Social Security Administration (SSA), private security companies, and State of Maine agencies.

5.0. Management Commitment

The State of Maine is committed to following this policy and the procedures that support it.

6.0. Coordination Among Agency Entities

OIT works with agencies to meet all State and Federal compliance requirements related to information security. OIT cooperatively assesses the security controls of information systems and their environments of operation, as outlined in this document, to determine the extent to which the controls are implemented correctly, are operating as intended, and are producing the desired outcome with respect to meeting established security requirements.

7.0. Compliance

7.1. For State of Maine employees, failure to comply with the procedures identified in this policy may result in progressive discipline, up to and including dismissal.

7.2. For non-State of Maine employees, failure to comply with the procedures identified in this policy may result in removal of the individual's ability to access and use State of Maine data and systems. Employers of non-State of Maine personnel will be notified of violations.

7.3. Personnel are also subject to penalties for violations of statutory compliance requirements. Depending on the requirement and the nature of the violation, penalties may include fines and criminal charges.

8.0. Procedures

The following security controls are established to meet an acceptable level of protection for State of Maine information systems. They serve as the base set of procedural requirements implemented to provide security assessment and authorization.

8.1. Security Assessment (CA-2, CA-2(1))

8.1.1. The Information Security Office works with agencies and other business units of OIT to facilitate the completion of Federal and State audits, remediate audit findings, and assist with the completion of associated documentation.

8.1.2. Planned onsite security control assessments and assessment report requirements that meet Federal statutory requirements are found in Appendix A – Federal Security Assessments. The onsite audits listed in this appendix are conducted by independent, third-party assessors.

8.1.3. Additional security authorizations are granted by standing governing bodies. These bodies develop data security standards for their respective services that are often used by State of Maine agencies. Security assessments and assessment report requirements that meet these established requirements are found in Appendix B – Governance Compliance Standards.

8.1.4. In addition to the audits and reports found in Appendix A, ad hoc security control assessments and assessment reports are determined by the Chief Information Security Officer (CISO), Chief Information Officer, and other State of Maine agencies. These assessments are usually conducted through contracts with professional service firms who are selected based on their ability to conduct impartial assessments. The scope of these assessments is based on needs at the time the firm is engaged. Professional service firm audits that involve OIT support must be approved by the CISO prior to contract approval.

8.1.5. Additional security assessments are conducted, including:

8.1.5.1. The Information Security Office conducts a self-assessment annually as a part of the Nationwide Cybersecurity Review (NCSR). The NCSR is a no-cost, anonymous, annual self-assessment designed to measure gaps and capabilities of state, local, tribal, and territorial governments' cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by the Department of Homeland Security and the Multi-State Information Sharing and Analysis Center.

8.1.5.2. The State of Maine conducts both routine (primarily through the Office of the State Auditor) security inspections as authorized by statute as well as ad hoc reviews (for example, Office of Program Evaluation and Government Accountability). The scope of these assessments varies, but they do provide OIT with findings related to security.

8.1.5.3. The Information Security Office and Network Security primarily conduct continuous monitoring and work with the other business units for remediation of findings.

8.1.5.4. Every 18 months, the Information Security Office coordinates with the State of Maine agencies that handle FTI for the completion of internal inspection of all OIT locations that contain FTI (excluding Federal Risk and Authorization Management Program–certified sites) to include:

8.1.5.4.1. Iron Mountain Inc., Scarborough, Maine

8.1.5.4.2. Sewall Street Data Center, Augusta, Maine
8.1.5.4.3. Commerce Street Data Center, Augusta, Maine
8.1.5.5. System development lifecycle activities assess risk as a part of both the deployment certification and change management processes (described in 8.4.2 below).

8.2. System Interconnections (CA-3, CA-3(5))

8.2.1. OIT documents system interconnections (see Definitions) with vendors using Service Level Agreements, Memorandums of Agreement, and contracts. The Data Exchange Policy[1] outlines requirements for data exchange and includes a template Memorandum of Agreement.

8.2.2. Interconnection documentation includes:
8.2.2.1. The technical and security requirements for establishing, operating, and maintaining the interconnection; and
8.2.2.2. The terms and conditions for sharing data, including the following:
8.2.2.2.1. The purpose of the interconnection;
8.2.2.2.2. Identification of the relevant authorities;
8.2.2.2.3. Specification of the responsibilities of both organizations; and
8.2.2.2.4. Definition of the terms of agreement including:
8.2.2.2.4.1. Apportionment of costs; and
8.2.2.2.4.2. The timeline for terminating or reauthorizing the interconnection.

8.2.3. OIT-managed firewalls universally enforce a deny-all-allow-by-exception rule for all external traffic seeking entry to the State network. Also, all access is universally secured by authentication credentials and is encrypted both at rest and in motion. See Access Control Policy and Procedures (AC-1)[2] for more information.

8.3. Plan of Action and Milestones (CA-5, CA-5(1))

8.3.1. The OIT process for Plan of Action and Milestones (POA&M) development and review is as follows:
8.3.1.1. Information Security Office maintains a consolidated POA&M. The consolidated POA&M is based on:
8.3.1.1.1. Audit results;
8.3.1.1.2. Gaps in policy and procedures; and
8.3.1.1.3. POA&M findings for certain Federal audits (for example, IRS, CMS, and SSA) for which OIT is responsible.
8.3.1.2. OIT reviews the consolidated POA&M with the CISO quarterly in the months of March, June, September, and December.

[1] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataExchangePolicy.pdf
[2] https://www.maine.gov/oit/policies/AccessControlPolicy.pdf

8.3.1.3. The POA&M includes corrective actions identified as necessary during the internal inspection outlined in Security Assessments (CA-2) above and identifies the actions OIT plans to take to resolve these findings. See the Plan of Action and Milestones Process[3] (PM-4) for more information.

8.3.1.4. Information Security Office employs automated mechanisms to ensure that the POA&M for the information system are accurate, up to date, and readily available.

8.3.2. Agencies may have to establish and maintain a POA&M for agency-level findings to meet regulatory compliance requirements.

8.4. **Security Authorization (CA-6)**

8.4.1. The Chief Information Officer is the senior-level executive, head of OIT, who serves as the authorizing official for applications and computer infrastructure for State of Maine agencies.

8.4.2. OIT partners with supported agencies to make the final determination whether applications and computer infrastructure are placed into production, based on the following OIT policies:

8.4.2.1. OIT Infrastructure Deployment Certification Policy[4]

8.4.2.2. OIT Application Deployment Certification Policy[5]

8.4.2.3. OIT Change Management Policy[6]

8.4.3. OIT change management procedures address, among other processes, system quality assurance development and change management testing. These documents outline the authorities and roles involved in the process of making a significant change to State of Maine infrastructure.

8.4.4. Agencies should develop and implement their own internal change management procedures.

8.4.5. See OIT System and Services Acquisition Policy and Procedures[7] (SA-1) for authorization requirements for information system changes that occur as a result of the acquisition process.

[3] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/ProgramManagementPolicy.pdf
[4] https://www.maine.gov/oit/policies/Infrastructure-Deployment-Certification.pdf
[5] https://www.maine.gov/oit/policies/Application-Deployment-Certification.pdf
[6] https://www.maine.gov/oit/policies/ChangeManagementPolicy.pdf
[7] https://www.maine.gov/oit/policies/SystemAndServicesAcquisitionPolicy.pdf

8.5. **Continuous Monitoring (CA-7, CA-7(1))**

8.5.1. OIT monitors all OIT-hosted information assets to detect attacks and indicators of potential attacks, as well as unauthorized local, network, and remote connections. A list of tools employed by OIT for continuous monitoring of the State of Maine network is included in the OIT Cyber Incident Response Plan[8] (IR-8) (Intranet only).

8.5.2. OIT performs continuous monitoring of OIT-hosted information systems, including:

8.5.2.1. Real-time scans at network entry and exit points to detect and eradicate malicious code (see Definitions);

8.5.2.2. Weekly scans of information systems and real-time scans of files from external sources;

8.5.2.3. Ongoing security control assessments; and

8.5.2.4. Internal security alerts, advisories, and directives generated by the Information Security Office and deemed necessary in response to a known issue, a known threat, or to strengthen the State's security posture.

8.5.3. OIT generates a monthly report that identifies the amount of spam (see Definitions) received by type: phishing (see Definitions), viruses, or nonrepudiation.

8.5.4. Response actions are managed through a POA&M (see section 8.33).

8.6. **Internal System Connections (CA-9)**

8.6.1. State of Maine employees and contractors are prohibited from connecting any new devices to any State of Maine network for any reason. For additional information, see the Network Device Management Policy[9].

8.6.2. No net-new, standing data exchange can commence without a signed Memorandum of Agreement (MoA) amongst the Authorized Custodians of the transacted data. Exempted are cases where both the sender and receiver happen to be the same authorized custodian. For additional details on Internal System Connections to include a sample data exchange MOA, see the Data Exchange Policy.[10]

8.7. **Financial Data on State Network**

8.7.1. All credit card transactions over the State Network must be encrypted end-to-end. According to PCI-DSS,[11]the State Network then functions as the

[8] http://inet.state.me.us/oit/policies/documents/IncidentResponsePlan.pdf
[9] https://www.maine.gov/oit/policies/NetworkDeviceManagementPolicy.pdf
[10] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/data-exchange-policy.pdf
[11] https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf

Internet Service Provider (ISP) and is not subject to any additional certification.

9.0. Document Details

9.1. Initial Issue Date: September 6, 2019
9.2. Latest Revision Date: September 4, 2024
9.3. Point of Contact: Enterprise.Architect@Maine.Gov
9.4. Approved By: Chief Information Officer, OIT
9.5. Legal Citation: Title 5, Chapter 163: Office of Information Technology[12]
9.6. Waiver Process: Waiver Policy[13]
9.7. Distribution: Internet[14]

10.0. Review

This document is reviewed triennially and when substantive changes are made to policies, procedures, or other authoritative regulations that affect it.

11.0. Records Management

Office of Information Technology security policies, plans, and procedures fall under the *Routine Administrative Policies and Procedures and Internal Control Policies and Directives* records management categories. They will be retained for three (3) years, and then destroyed in accordance with guidance provided by Maine State Archives. Retention of these documents will be subject to any future State Archives General Schedule revisions that cover these categories.

12.0. Public Records Exceptions

Under the Maine Freedom of Access Act (FOAA), certain public records exceptions may limit disclosure of agency records related to information technology infrastructure and systems, as well as security plans, procedures, or risk assessments. Information contained in these records may be disclosed to the Legislature, or, in the case of a political or administrative subdivision, to municipal officials or board members under conditions that protect the information from further disclosure. Any aggrieved person seeking relief for an alleged violation of the FOAA may bring suit in any Superior Court in the state.

13.0. Definitions

13.1. Federal Tax Information (FTI): Federal tax returns and return information (and information derived from it) that is in the agency's possession or control which is received directly from the IRS (or obtained through an authorized secondary source), covered by the confidentiality protections of the Internal Revenue Code (IRC), and subject to the IRC 6103(p)(4) safeguarding requirements including IRS

[12] https://legislature.maine.gov/statutes/5/title5ch163sec0.html
[13] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/waiver.pdf
[14] https://www.maine.gov/oit/policies-standards

oversight. FTI may contain Personally Identifiable Information (PII) IRS Publication 1075.[15]

13.2. Information asset*:* A discrete, identifiable piece of information technology, including hardware, software, and firmware. Information assets include, for example, mainframes, workstations, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), input/output devices (e.g., scanners, copiers, printers), network components (e.g., firewalls, routers, gateways, voice and data switches, process controllers, wireless access points, network appliances, sensors), operating systems, virtual machines, middleware, business applications, system software, development tools, and miscellaneous related utilities.

13.3. Malicious code: Unwanted files or programs that can cause harm to a computer or compromise data stored on a computer. Classifications of malicious code include viruses, worms, and Trojan horses.

13.4. Phishing: The practice of sending fraudulent communications that appear to come from a reliable source, usually through email, with the goal of stealing data, such as credit card or login information, or to install malware on the recipient's machine.

13.5. Spam: Unsolicited usually commercial messages (such as emails, text messages, or internet postings) sent to a large number of recipients or posted in a large number of places.

13.6. System interconnection: The direct connection of two or more information technology systems for the purpose of sharing data and other information resources.

14.0. Abbreviations

14.1. ACA: Affordable Care Act
14.2. ACH: Automated Clearing House
14.3. CAP: Corrective Action Plan
14.4. CS: Child Support
14.5. CISO: Chief Information Security Officer
14.6. CJIS: Criminal Justice Information System
14.7. CMS: Centers for Medicare & Medicaid Services
14.8. U.S. DHHS: U.S. Department of Health and Human Services
14.9. FBI: Federal Bureau of Investigation
14.10. FEDRAMP: Federal Risk and Authorization Management Program
14.11. FOAA: [Maine] Freedom of Access Act
14.12. FPLS: Federal Parent Locator Service
14.13. FTI: Federal Tax Information
14.14. HIPAA: Health Insurance Portability and Accountability Act

[15] https://www.irs.gov/pub/irs-pdf/p1075.pdf

14.15. IRC: Internal Revenue Code
14.16. IRS: Internal Revenue Service
14.17. ISP: Internet Service Provider
14.18. NACHA: National Automated Clearing House Association
14.19. NCSR: Nationwide Cybersecurity Review
14.20. OCR: [U.S. Department of Health and Human Services] Office for Civil Rights
14.21. OCSE: Office of Child Support Enforcement
14.22. ODFI: Originating Depository Financial Institution
14.23. OIT: Office of Information Technology
14.24. PCI DSS: Payment Card Industry Data Security Standard
14.25. POA&M: Plan of Action and Milestones
14.26. SAQ: Self-Assessment Questionnaire
14.27. SCA: Security Controls Assessment
14.28. SSA: Social Security Administration
14.29. SSR: Safeguard Review Report

Appendix A – Federal Security Assessments

1.0 Internal Revenue Service–Related Items

1.1. Reference: Internal Revenue Service (IRS) Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies.

1.2. IRS Office of Safeguards Onsite Review – Every three years, the IRS assesses all security controls and enhancements during an onsite review of all agencies that receive, process, or store Federal Tax Information (FTI). The team from IRS Office of Safeguards uses both testing and interviewing assessment methods. The IRS issues a Safeguard Review Report (SRR) and a Corrective Action Plan (CAP) to document its onsite review findings.

1.3. Safeguard Security Report (SSR) Development – Agencies that receive FTI (Maine Revenue Services, the Department of Labor, and Department of Health and Human Services) provide the IRS with a self-assessment of the current state of their information security in the SSR. Agencies that receive FTI submit a yearly update (due May 30) of the SSR, which is accompanied by a certification of accuracy signed by the appropriate director. The SSR uses interviewing assessment methods and addresses all security controls and enhancements.

1.4. CAP Development – Agencies that receive FTI submit an updated CAP semi-annually: (i) as an attachment to the SSR on May 30 and (ii) separately on the CAP due date, November 30. The CAP assesses all security control deficiencies identified during the IRS onsite audit. For outstanding findings, agencies that receive FTI list actions taken, or planned, to implement recommendations from the SRR issued as the result of an IRS onsite review. Supporting documentation is required to close any finding identified as a critical or significant risk to FTI. The IRS tracks all review findings in a database until the findings are closed with an implementation date via the CAP update process. OIT is responsible for corrective action plans and remediation of all select findings (in other words, tab H) and any physical findings on OIT locations or data centers.

1.5. Internal Inspection

1.5.1. The IRS requires internal inspections by the agencies that receive, process, or store FTI in order to ensure that the security policies and procedures established by the agency to protect FTI are functioning, being maintained, and being enforced. The inspection of OIT facilities is conducted every 18 months. Even though this internal inspection is focused on the security of FTI, it provides OIT an objective assessment of information security for all OIT facilities and has applicability beyond FTI.

1.5.2. The IRS also requires inspection of vendors that handle FTI for an agency not certified by the Federal Risk and Authorization Management Program (FEDRAMP), (cloud computing approval authority). The Iron Mountain

facility stores backup tapes of OIT data, including FTI data. External inspections are done to ensure that the security policies and procedures established by the vendor to protect FTI are functioning, maintained, and enforced. External inspections are conducted every 18 months. One of the agencies using a vendor is required to conduct the inspection and provide the inspection report to the other agencies.

2.0 Social Security Administration

2.1. Reference: Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration (SSA).

2.2. SSA Onsite Compliance Review – Every three years, the SSA assesses all security controls and enhancements during an onsite review of all agencies that receive, process, or store SSA Information. The SSA uses both testing and interviewing assessment methods, and it issues a formal report to document its onsite review findings. Updates to these findings are due to the SSA quarterly until resolved.

2.3. Compliance Review Questionnaire – Agencies that receive information from the SSA submit an updated Compliance Review Questionnaire every three years prior to the Onsite Compliance Review. The Compliance Review Questionnaire describes the management, operational, and technical controls used to protect SSA-provided information from misuse and improper disclosure.

3.0 Federal Bureau of Investigation

3.1. Reference: CJISD-ITS-DOC-08140-5.7, Criminal Justice Information Services (CJIS) Security Policy.

3.2. CJIS Onsite Security Inspection – At a minimum, the CJIS audit manager audits all agencies and contractors with access to federally provided criminal justice information every three years. The FBI uses direct access to the State system to ensure compliance with applicable statutes, regulations, and policies.

3.3. CJIS Preaudit Questionnaire – A few months before the CJIS audit is conducted, the State of Maine receives a preaudit questionnaire. The preaudit questionnaire is used to assist the audit manager in gathering pertinent information prior to the onsite visit. Information gathered from the preaudit questionnaire is used to formulate additional questions to be answered during the onsite visit and to assist in determining policy compliance.

4.0 Centers for Medicare & Medicaid Services

4.1. Reference: MARS-E Document Suite, Version 2.0 Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges.

4.2. Minimal Acceptable Risk Standards for Exchange (MARS-E) 2.0 Security Controls Assessment (SCA) - At a minimum, CMS requires an onsite security controls assessment be conducted every three years by CMS, or by an approved third party, for all agencies with access to federally provided Affordable Care Act (ACA) data. The SCA includes the examination of documents, settings, configurations, controls, interviews of organizational personnel, and technical testing. The purpose of a SCA is to determine whether security and privacy controls are implemented correctly, operate as intended, and produce the desired outcomes for meeting the security and privacy requirements of the information system.

4.3. Security and Privacy Controls Assessment Test Plan – The Security and Privacy Controls Assessment Test Plan documents all testing to be conducted during the assessment to validate the security and privacy controls for agencies with access to ACA data.

4.4. ACA Administering Entity System Security Plan – The System Security Plan documents compliance with mandates of the ACA legislation and DHHS regulations for agencies that receive ACA data. The System Security Plan is the key tool for describing the information technology security and privacy environment for information technology systems and for documenting the implementation of security and privacy controls for the protection of all data received, stored, processed, and transmitted by the ACA information technology systems and supporting applications. The System Security Plan must be initiated during the initial stages of the life cycle process for information technology systems and maintained thereafter.

4.5. Security Assessment Report - At the completion of the SCA, the assessor provides a Security Assessment Report that presents the findings of the assessment annotated in detail with the remediation recommendations for the weaknesses or deficiencies found in the information system security controls implementation. Findings in the Security Assessment Report must be reported and monitored until they are remediated in a Plan of Action and Milestones.

5.0 U.S. Department of Health and Human Service Office for Civil Rights

5.1. References

5.1.1. U.S. DHHS Audit Protocol, July 2018;

5.1.2. HIPAA Security Series, Volume 2, Paper 1 through 7; and

5.1.3. HIPAA Privacy, Security, and Breach Notification Audit Program, hhs.gov

5.2. Desk Audits – The Office for Civil Rights (OCR) expects covered entities that are the subject of an audit to submit requested information via OCR's secure portal within 10 business days of the date on the information request. After the documents are received, the auditor will review the information submitted and provide the auditee with draft findings. Auditees will have 10 business days to review and return

written comments, if any, to the auditor. The auditor will complete a final audit report for each entity within 30 business days after the auditee's response. OCR will share a copy of the final report with the audited entity.

5.3. Onsite Audits – Similarly, entities will be notified via email of their selection for an onsite audit. The auditors will schedule an entrance conference and provide more information about the onsite audit process and the expectations for the audit. Each onsite audit will be conducted over a period of three to five days, depending on the size of the entity. Onsite audits are more comprehensive than desk audits and cover a wider range of requirements from the HIPAA rules. As with desk audits, entities will have 10 business days to review the draft findings and provide written comments to the auditor. The auditor will complete a final audit report for each entity within 30 business days after the auditee's response. OCR will share a copy of the final report with the audited entity.

6.0 Office of Child Support Enforcement

6.1. Reference: Security Agreement between the U.S. Department of Health and Human Services Administration of Children and Families Office of Child Support Enforcement (OCSE) and the State Agency Administering the Child Support Program

6.2. The federal Office of Child Support Enforcement selects Child Support (CS) program agencies throughout the year for safeguard reviews to assess their security posture for safeguarding the National Directory of New Hires information, Federal Parent Locator Service (FPLS) information and Child Support program information which is received for authorized purposes via the Security Agreement. If an agency is selected for a safeguard review, it will receive email notification with additional information from the OCSE.

Appendix B – Governance Compliance Standards

1.0 Payment Card Industry Data Security Standard (PCI DSS)

1.1. Reference: PCI Security Standards Council Website.[16]

1.2. Self-Assessment – State of Maine agencies that use credit card data must complete a Self-Assessment Questionnaire (SAQ) annually to maintain compliance. The SAQ utilized is based on the type and amount of credit card transactions conducted by an agency. OIT cannot answer infrastructure questions on the SAQ because it operates essentially as an internet service provider and the transitions may only use PCI DSS compliant devices that provide end to end encryption of the credit card information.

1.3. Remote Penetration Testing - Based on the type and amount of credit card transactions conducted by an agency, a penetration test may be conducted based on the IP address utilized. If the test is conducted against the State of Maine network, the results will show the perimeter security is working designed.

2.0 National Automated Clearing House Association (NACHA)

2.1. References

2.1.1. NACHA Operating Rules and Guidelines; and

2.1.2. ACH Compliance Manual

2.2. Each Originating Depository Financial Institution (ODFI) (typically a bank) is responsible for ensuring that its Originators (i.e., State of Maine agencies conducting ACH transactions) adopt and implement commercially reasonable policies, procedures, and systems to receive store, transmit, and destroy consumer-level ACH data in a secure manner and to protect against data breaches.

2.3. The annual Rules Compliance Audit applies directly to ODFIs, but not directly to Originators. That is because Originators are bound through their origination agreements with their ODFI.

2.4. Care must be taking when establishing the origination agreements with an ODFI through the contracting process to ensure commercial reasonableness is maintained. Specifically, an agency cannot commit to on-site audits or other security assessments without the express approval of the Chief Information Security Officer.

[16] https://www.pcisecuritystandards.org/