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

---

## System and Communications Protection Procedures for Defense in Depth (SC-2, 4, 5, 20, 21, 22, 23, 28, 32, and 39)

---

## Table of Contents

## 1.0. Purpose

These procedures identify how the State of Maine (SOM) meets security requirements pertaining to application partitioning, information in shared resources, denial of service protection, name/address resolution, session authenticity, information at rest, information system partitioning, and process isolation. This document corresponds to the System and Communications Protection Controls SC-2, 4, 5, 20, 21, 23, 28, 32, and 39 of the SC Family of National Institute of Standards and Technology (NIST) Special Publication 800-53.

## 2.0. Scope

2.1. These procedures apply 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 (see Definitions), irrespective of location; and

2.1.2. Information assets from other State government branches that use Executive Branch managed services.

## 3.0. Conflict

If these procedures conflict with any law or union contract in effect, the terms of the existing law or contract prevail.

## 4.0. Procedures

4.1. Controls Cross References: The following controls for the System and Communications Protection Policy and Procedures (SC) are published in separate policy and procedure documents:

4.1.1. System and Communications Protection Policy and Procedures (SC-1, 7, 8);[1]

4.1.2. System and Communications Protection Procedures for Encryption Mechanisms (SC-12, 13, and 17);[2] and

4.1.3. System and Communications Protection Procedures for Specific Technologies (SC-6, 10, 15, 18, 19, 40).

### 4.2. Application Partitioning (SC-2)

4.2.1. Application partitioning ensures information systems separate user functionality (including user interface services) from information system management functionality.

4.2.2. Office of Information Technology (OIT) Information Asset Owners separate user functionality, including user interface services, from information system management functionality using Advanced Encryption Standard (AES) 256 (see Definitions), which is compliant with Federal Information Processing Standard (FIPS)[3] (see Definitions) 140-2.

4.2.3. OIT Information Asset Owners ensure that administrative options are not available to non-privileged (see Definitions) users, including options that are

[1] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/SystemCommunicationsProtectionPolicy.pdf
[2] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/SCEncryptionMechanismsProcedures.pdf
[3] https://csrc.nist.gov/publications/detail/fips/140/2/final

greyed out, until user sessions are established with administrator privileges. See Access Control Procedures for Users (AC-2).[4]

4.2.4. OIT uses the following methods to separate user functionality from information system management functionality:

4.2.4.1. Active Directory (AD) permissions restrict a user's ability to access or start up an application.

4.2.4.2. Application user accounts are required for successful login.

4.2.4.3. Role-based access control (RBAC) (see Definitions) allows user access, as-needed, based on the user's role. Restrictions for RBAC are associated with data governed by federal entities and laws such as the Internal Revenue Service, U.S. Department of the Treasury, Social Security Administration, and Health Insurance Portability and Accountability Act.

## 4.3. Information in Shared Resources (SC-4)

4.3.1. Information Asset Owners ensure that information systems prevent unauthorized and unintended information transfer via shared system resources using the following methods:

4.3.1.1. Logical and physical segregation of the data;

4.3.1.2. Implementation of RBAC;

4.3.1.3. Continuous monitoring, audit, and accountability procedures; and

4.3.1.4. Data exchanges, documented to include roles and responsibilities for information security (see the Data Exchange Policy).[5]

## 4.4. Denial of Service Protection (SC-5)

4.4.1. OIT Network Security prevents Denial of Service (DoS) attacks (see Definitions) against web assets using a Web Application Firewall (WAF) as a cloud reverse-proxy to conceal the Internet Protocol (IP) addresses of web servers. The WAF:

4.4.1.1. Filters malicious traffic before it reaches the web servers;

4.4.1.2. Leverages a global Content Delivery Network (see Definitions) for geographic redundancy; and

4.4.1.3. Provides unlimited distributed denial-of-service (DDoS) (see Definitions) protection.

4.4.2. OIT Network Security uses Network Visibility & Analytics Software for DoS protection using enterprise telemetry from the existing network infrastructure.

4.4.3. SOM firewalls are configured to fail securely (closed) to prevent further traffic and operation when DoS attack conditions are detected.

4.4.4. In the event of a DDoS alert or attack, OIT Network Operations or Information Security Office will submit a report of the situation to Networkmaine. The University of Maine System, via Networkmaine, uses Akamai DDoS Attack Prevention. Upon detection and validation of a DDoS

[4] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/AccessControlProceduresForUsers.pdf

[5] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataExchangePolicy.pdf

attack, Akamai DDoS Attack Prevention will have the traffic externally scrubbed.

4.4.5. The types, appropriate tools, and procedures for responding to DoS attacks are detailed in the Cyber Incident Response Plan[6] (Intranet only).

## 4.5. Secure Name/Address Resolution (Authoritative Source) (SC-20)

4.5.1. OIT Network Security utilizes an Internet Protocol Address Manager (IPAM) to provide a secure domain name system resolution for data origin authentication and integrity verification artifacts.

4.5.1.1. The exchange is accomplished via its distributed grid to defend against a wide range of external and internal Domain Name System (DNS)-based attacks such as floods, exploits, DNS hijacking, and data exfiltration.

4.5.1.2. The IPAM grid members securely exchange information over Virtual Private Network (VPN) connections.

4.5.2. The IPAM validates authoritative name resolution requests received via a query on the back end to OIT's AD which is returned by the system in response to external name/address resolution queries.

4.5.3. The IPAM DNS secure server enables verification of a chain of trust (see Definitions) among parent and child zones, if the child zone supports secure resolution services when operating as part of a distributed, hierarchical namespace.

## 4.6. Secure Name/Address Resolution (Recursive or Caching Resolver) (SC-21)

4.6.1. OIT Network Security utilizes DNS servers, which are Authoritative for the Maine.Gov domain that securely provides DNS for zones delegated by the DotGov registrar (see Definitions).

4.6.2. The Secure DNS (SDNS) servers locate external DNS names through queries to other external nameservers via recursive or caching resolver.

4.6.3. OIT Network Security utilizes access control lists, populated by other DNS server names, that allow access only from a specified list of outside DNS servers. This method prevents unauthorized use of DNS infrastructure as an open resolver for recursive queries (see Definitions).

## 4.7. Architecture and Provisioning for Name/Address Resolution Service (SC-22)

4.7.1. OIT Network Security employs a distributed grid of IPAM appliances with the separation of internal and external roles to ensure redundancy and fault tolerance.

4.7.2. The authoritative pair of IPAM appliances are hosted internally and located in the SOM's two principal data centers.

4.7.3. Two Authoritative name servers for external DNS are deployed in a primary/secondary configuration, where firewalls allow internal requests

[6] http://inet.state.me.us/oit/policies/documents/IncidentResponsePlan.pdf

from clients which mitigates the impact of hardware failure of individual units.

## 4.8. Session Authenticity (SC-23)

4.8.1. OIT Network Security implements session-level mechanisms to protect communication integrity, confidentiality, and authenticity against man-in-the-middle attacks (see Definitions). These types of attacks include session hijacking and the insertion of false information into session transmissions that are in alignment with vender-provided defaults, i.e., middleware, Linux, and Active Directory.

4.8.2. The OIT Computing Infrastructure & Services team in collaboration with the Unix, Oracle Database, and Middleware teams implement session authenticity mechanisms that align with both governing and regulatory bodies. An example of OIT's authenticity mechanisms may include Transport Layer Security, multi-factor authentication, VPNs, digital time signatures, and digital time stamping.

4.8.3. **Invalidate Session Identifiers at Logout (SC-23(1)):** OIT Network Security implements automatic session lockouts to systems and applications, once a user logs out of a workstation, through mechanisms such as a Failsafe Central Management System, which is a cyber guard for both internal and external session-level protection.

4.8.4. **Allowed Certificate Authorities (SC-23(5)):** Public Key Infrastructure (PKI) Certificate Authorities (CAs) adhere to all standard best practices, spanning Microsoft, Oracle, and Red Hat Enterprise Linux AD Certificate Services and are built into OIT's AD.

4.8.4.1. OIT maintains a process to strictly control PKI-based authentication. See the Identification and Authentication Policy and Procedures (IA-1)[7] (Intranet only).

4.8.4.2. The following PKI Certificates are utilized by OIT:

4.8.4.2.1. Entrust provides CAs to ensure authenticity of external electronic communications such as digital signing and email encryption.

4.8.4.2.2. SOM Root CA provides internal-only CA services to ensure the authenticity of servers and network devices provisioned by SOM along with CA services for internal website and service encryption.

4.8.4.3. In general, exportation of the PKI private key is prohibited. See 8.4.6.1. of Configuration Management Policy[8] for permitted use cases.

## 4.9. Protection of Information at Rest (SC-28)

4.9.1. The OIT Computing Infrastructure and Services team, in collaboration with the OIT Oracle Database team, protects the confidentiality and integrity of

[7] https://inet.state.me.us/oit/policies/documents/IdentificationAuthenticationPolicy.pdf

[8] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/ConfigurationManagementPolicy.pdf

data at rest (see Definitions) through user privileges, database encryption, file-server encryption, and storage mechanisms.

4.9.2. OIT has adopted the Traffic Light Protocol (TLP) as the method for classifying data (see the Data Classification Policy[9]). All data/information identified as TLP: Amber or TLP: Red is encrypted at rest using AES 256 encryption to prevent unauthorized disclosures and modifications.

4.9.3. Virtual database storage is employed by default through a relational database management system. This system hosts multiple levels of encryption to protect TLP: Amber and TLP: Red data at rest.

4.9.4. All offline storage network shares for legacy assets containing TLP: Amber or TLP: Red data are secured and backed up in alignment with the Media Protection Policy (MP-1)[10] (Intranet only). The legacy Commvault system is used to maintain and store tape backups offsite at Iron Mountain.

4.9.5. Agencies, in consultation with OIT, ensure approved authorizations to information and system resources are enforced through access enforcement, separation of duties, and principle of least privilege (see Access Control Procedures for Users[11]).

4.9.6. Agencies, in consultation with OIT, ensure that integrity verification tools are employed to detect unauthorized changes to software and information (see System and Information Integrity Policy and Procedures (SI-1)[12]).

## 4.10. Information System Partitioning (SC-32)

4.10.1. The OIT Information Security Office utilizes Cisco AnyConnect, Cisco Tetration, and Cisco ISE for visibility into how endpoints (see Definitions) access applications in SOM's data centers and to allow macro-segmentation (see Definitions) at the firewall layer. The logic and granularity of the segmentation is determined by the CISO, based upon the data classification of the underlying information assets, regulatory compliance, business needs, and other architectural and cybersecurity considerations. Servers are placed inside a certain network range of OIT's data centers to control ingress and egress mechanisms from targeting or hacking into specific zones and servers.

4.10.2. Datacenter firewalls provide broader information system partitioning.

4.10.3. Cisco's ISE runs on all user-connecting switches with business policy rules that determine which systems can communicate. Currently, segmentation is based upon identity and access control pegged to the enterprise Active Directory.

4.10.4. OIT data labeling follows the Traffic Light Protocol taxonomy to determine the appropriate classification of data and to inform segmentation efforts. See the Data Classification Policy.[13]

---

[9] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataClassificationPolicy.pdf
[10] https://inet.state.me.us/oit/policies/documents/MediaProtectionPolicy.pdf
[11] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/AccessControlProceduresForUsers.pdf
[12] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/SystemInformationIntegrityPolicy.pdf
[13] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataClassificationPolicy.pdf

4.10.5. Internet protocol address space is defined for systems by logical domains that are live on the SOM network.
4.10.6. Physical security of information systems in the data centers are detailed in the Physical and Environmental Protection Policy and Procedures[14] (PE-1).

4.11. **Process Isolation (SC-39)**
4.11.1. The OIT Computing Infrastructure & Services team, in collaboration with the OIT Oracle Database team, maintains a separate execution domain for each executing process.
4.11.2. Separation for Process Isolation: The OIT Computing Infrastructure & Services team, in collaboration with the OIT Linux team, utilizes Linux Kernel Features, Namespaces, Control Groups (Cgroups) (see Definitions), and Capabilities to maintain separate execution domains as well as Microsoft Distribution Points (DP) and Data Execution Prevention (DEP). The Microsoft Data Execution Policy is on by default in Windows 10 and Microsoft server 2016 and newer.
4.11.2.1. Microsoft DEP is used during process isolation as well as to perform additional checks on memory to prevent malicious code from running on the system.
4.11.2.2. Namespaces maintain a separate execution domain that is only visible to other Namespace processes.
4.11.2.3. Cgroups are provided through a pseudo-filesystem and implemented in the core Cgroup kernel code, while resource tracking, and limits are implemented in a set of per-resource-type subsystems such as memory and the central processing unit (CPU).
4.11.2.4. Capabilities is a per-thread attribute that divides the privileges associated with a privileged user (see Definitions) into distinct units to independently enable and disable domains.
4.11.2.5. Thread Isolation:
4.11.2.5.1. Linux Kernel Control Groups or Cgroups and Capabilities are used by OIT for thread isolation.
4.11.2.5.2. Microsoft DEP facilitates the control of process creep.

## 5.0. Document Details

5.1. Initial Issue Date: 30 January 2024
5.2. Latest Revision Date: 20 March 2024
5.3. Point of Contact: Enterprise.Architect@Maine.Gov
5.4. Approved By: Chief Information Officer, OIT
5.5. Legal Citation: Title 5, Chapter 163: Office of Information Technology[15]
5.6. Waiver Process: Waiver Policy[16]
5.7. Distribution: Internet[17]

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

## 6.0. Review

This document will be reviewed triennially, and whenever substantive changes are made to Policies, Procedures, or other authoritative regulations affecting this document.

## 7.0. Records Management

OIT major policies and procedures fall under Maine State Archives General Schedule 1, Administrative Records[18], series GS1.13a, Policies and Procedures – Major. They will be retained for 6 years after being superseded or withdrawn. Typically, these records are archival (permanent) value, and will be evaluated on a case-by-case basis by Maine State Archives staff. If deemed archival (permanent) value, then OIT should send these records to Maine State Archives for their historical/research collection.

## 8.0. 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.

## 9.0. Definitions

9.1. Advanced Encryption Standard (AES) 256: A U.S. Government-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Source NIST.[19]

9.2. Chain of Trust: A certain level of trust in supply chain interactions such that each participant in the consumer-provider relationship provides adequate protection for its component products, systems, and services. Source NIST.[20]

9.3. Content Delivery Network: A network of servers that is geographically dispersed to enable faster web performance by locating copies of web content closer to users or facilitating delivery of dynamic content (e.g., live video feeds).

9.4. Control Group (Cgroup): A Linux kernel feature that limits, accounts for, and isolates the resource usage (CPU, memory, disk I/O, network, etc.) of a collection of processes.

[18] https://www.maine.gov/sos/arc/records/state/GS1Administrative.pdf
[19] https://csrc.nist.gov/glossary/term/advanced_encryption_standard
[20] https://csrc.nist.gov/glossary/term/chain_of_trust

9.5. Data at Rest: The state of information when it is located on storage devices as specific components of information systems.

9.6. Denial of Service (DoS) Attack: The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided). Source NIST.[21]

9.7. Distributed Denial of Service (DDoS) Attack: A denial of service technique that uses numerous hosts to perform the attack. Source NIST.[22]

9.8. DotGov Registrar: The domain name '.gov' is a sponsored top-level domain (sTLD) in the Domain Name System of the Internet. DotGov is derived from the word government, indicating its restricted use by government entities. The TLD is administered by the Cybersecurity and Infrastructure Security Agency (CISA), which is a component of the United States Department of Homeland Security.

9.9. Endpoints: End-user devices such as desktops, laptops, and mobile devices. Endpoints serve as points of access to an enterprise network and create points of entry that can be exploited by malicious actors.

9.10. Federal Information Processing Standard (FIPS): Publicly announced standards for use in computer systems by non-military American government agencies and government contractors.

9.11. Information Asset: a discrete, identifiable piece of information technology, including hardware, software, firmware, systems, services, and related technology assets used to execute work on behalf of OIT or another State Agency.

9.12. Macro-segmentation: A checkpoint software that allows an organization to inspect internal data flows at segment boundaries. This increases the probability of detecting this lateral movement. Macro-segmentation allows an organization to segment a network based on its business needs.

9.13. Non-Privileged User: A user who is unauthorized to perform security-relevant functions within various user accounts and processes.

9.14. Man-in-the-Middle Attack: An attacker positioned between two communicating parties in order to intercept and/or alter data traveling between them, for example, in the context of authentication, the attacker would be positioned between a claimant and a verifier during authenticator binding.

9.15. Privileged User: A user who is granted rights that go beyond those of a typical

[21] https://csrc.nist.gov/glossary/term/denial_of_service
[22] https://csrc.nist.gov/glossary/term/distributed_denial_of_service

business user to manage and maintain IT systems. Usually, these rights include administrative access to networks and devices and are separate from users' administrative access to their own workstations.

9.16. Recursive Query: A DNS query in which a resolver contacts a name server to perform a name lookup. The name server then returns a result or an error. The name server cannot refer the client to a different name server, but it can forward the query directly to another name server if it has a forwarder configured.

9.17. Role-Based Access Control (RBAC): Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals. Source NIST. [23]

## 10.0. Abbreviations

10.1. AD: Active Directory
10.2. AES: Advanced Encryption Standard
10.3. CA: Certificate Authority
10.4. Cgroup: Control Group
10.5. CPU: Central Processing Unit
10.6. DDoS: Distributed Denial of Service Attack
10.7. DEP: Data Execution Prevention
10.8. DoS: Denial of Service Attack
10.9. DNS: Domain Name System
10.10. DP: Distribution Points
10.11. FIPS: Federal Information Processing Standard
10.12. FOAA: Freedom of Access Act (Maine)
10.13. IP: Internet Protocol
10.14. IPAM: Internet Protocol Address Manager
10.15. ISE: Identity Services Engine (Cisco)
10.16. NIS: National Institute of Standards and Technology
10.17. OIT: Office of Information Technology
10.18. PKI: Public Key Infrastructure
10.19. RBAC: Role-Based Access Control
10.20. SC: System and Communications Protection
10.21. SDNS: Secure DNS
10.22. SOM: State of Maine
10.23. TLP: Traffic Light Protocol
10.24. WAF: Web Application Firewall
10.25. VPN: Virtual Private Network

[23] https://csrc.nist.gov/glossary/term/role_based_access_control