State of Maryland

STANDARD

SYSTEM & COMMUNICATION PROTECTION

Document No.	Last Updated	Prepared By
MD-STD-318-SC-01	02/18/2026	DOIT OSM

System and communication protection is a critical component of the Zero Trust Architecture (ZTA) framework by enforcing security through continuous verification, least privilege access, and micro-segmentation that protects systems and communications against unauthorized access and lateral movement.

PURPOSE AND SCOPE

Purpose	This standard provides the technical and operational specifications needed to prevent unauthorized access, detect threats and secure State data.
Scope	This standard addresses network security, boundary protection, transmission security, and access control for communications.
Applicability	This standard applies to all units of State government (as defined in SF&P 3.5-101(g)), hereafter referred to simply as "agencies."
Related Policy	This standard is part of a broader policy suite. Refer to MD-POL-100 Cybersecurity & Governance Policy, Appendix C for a list of related policies and standards.
Baseline	This standard has been developed using National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5 Moderate Baseline[1] and State-specific organizationally defined parameters. Agencies may be required to deviate from this baseline when State statute, executive orders, or applicable regulations establish a conflicting requirement that precludes compliance.
Distribution	This document is approved for public distribution and may be shared with external stakeholders, partners, and regulatory bodies. It reflects the State's commitment to transparency, compliance, and operational excellence. Unauthorized modifications or misrepresentation of this document are strictly prohibited.

[1] NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations.

FOREWARD

Agencies that use Department of Information Technology DoIT-managed services automatically receive, or *inherit*, the compliance those services already meet, reducing duplicative work and accelerating their overall compliance efforts. These centrally governed services, such as hosting platforms, identity management, and network infrastructure, are built with robust control frameworks that automatically extend to participating agencies. By leveraging these offerings, agencies not only align with key operational and security standards but also benefit from pre-configured environments, continuous monitoring, and policy enforcement mechanisms maintained by DoIT. Agencies are encouraged to leverage these services to accelerate readiness, gain cost efficiency, simplify compliance efforts, and allow agencies to focus more fully on mission delivery, knowing that foundational requirements are already in place. Agencies should review the scope of each managed service to understand which standards are inherited and where additional agency-specific controls may still be required.

GUIDANCE AND ENFORCEABILITY

Throughout this document, informational call-out boxes are utilized to provide additional context or elaborate on key topics. While these boxes primarily serve an informational purpose, any directives or mandated actions contained within them are authoritative and carry the same enforceability as the core requirements of this document. For the purposes of this document, the term “shall” denotes a mandatory requirement. Terms such as “where feasible”, “encouraged”, or similar phrasing indicate recommended practices that reflect organizational preference but are not enforceable requirements at this time.

CHANGE RECORD

Version	Summary of Changes	Changed By	Date
1.0	Initial Publication	Miheer Khona	02/18/2026

STANDARDS

318 State Strategy

These standards establish a baseline of system and communication protection practices that each agency must implement to comply with State cybersecurity and privacy policies. Each agency shall designate specific personnel with IT responsibilities to ensure the effective implementation of these standards.

318-1 Develop Agency-Level Procedures (SA-1)

In alignment with this standard, develop and document agency-level system and communication protection procedures. Agencies must disseminate the procedures to agency personnel with information technology (IT) security responsibilities. Agencies must review, and if needed, update the procedures as deemed appropriate by the agency based on changes and risk at least every **3 years**. Procedures must address purpose, scope, roles and responsibilities.

Zero Trust Architecture

For IT under agency control, the following foundational components of ZTA should be implemented where feasible: a) Network segmentation (e.g., maximize micro-segmentation); b) Network traffic management (e.g., dynamic network rules and configurations); c) Traffic encryption (e.g., all internal and maximize external); d) Network reliance (e.g., dynamically manage availability for major applications); e) Visibility and analytics (e.g., anomaly-based detection); and f) Automation and orchestration (e.g., automated change management and policy enforcement). Additional implementation guidance for each of these components is published by the NIST, Cybersecurity and Infrastructure Security Agency (CISA), International Organization for Standardization (ISO), and Institute of Electrical and Electronics Engineers (IEEE).

318-2 Separate System and User Functionality (SC-2)

Separate user functionality, including user interface services, from system management functionality. Separation may be accomplished using the following examples:

- Different computers;
- Different central processing units;
- Different instances of the operating system; or
- Different network addresses.

318-3 Protect Shared System Resources (SC-4)

Prevent unauthorized and unintended information transfer via shared system resources by properly removing data remnants as defined by *NIST Special Publication 800-88, Guidelines for Media Sanitization*.

318-4 Protect Against Denial-of-Service (SC-5)

Protect against the effects of denial-of-service (DoS) attacks by employing the following controls:

- Monitoring and controlling the total number of user sessions opened;
- Limited the total number of concurrent sessions that can be opened by a single user;
- Limiting the amount of idle time to **15 minutes** before the user session is forced to terminate; and
- Monitoring and controlling the number of concurrent, remote access sessions (including virtual private network (VPN), Secure Access Service Edge (SASE), Security Service Edge (SSE)) that can be opened by a single user to one (1).

Protect against the effects of and distributed DoS (DDoS) attacks by employing the following controls:

- Traffic anomaly detection;
- Rate limiting and throttling:
- Geo/IP filtering;
- Content Delivery Network (CDN) or scrubbing services; and/or
- Redundancy and failover.

318-5 Implement Boundary Protection (SC-7)

Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system; Implement subnetworks for publicly accessible system components that are either physically or logically separated from internal organizational networks; and Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

All inbound and outbound connections originating from or terminating in international locations shall be blocked by default unless the connection is explicitly authorized by the appropriate Authorizing Official based on a documented business need.

Logical Separation and Micro-Segmentation

To implement ZTA methodologies for boundary protection, where feasible, leverage boundary protection devices to enforce full logical separation State systems from non-organizational IT systems within the same infrastructure; b) Make multiple State systems within the same infrastructure readily distinguishable (from neighboring IT systems) by the underlying service or infrastructure provider (e.g., device naming scheme, logical addressing, segmentation); and c) Use micro-segmentation to the degree that is practical for the target environment. For example, a larger infrastructure should consider ideal areas for micro-segmentation, whereas a Software as a Service (SaaS) implementation may have no micro-segmentation at the tenant application level (even though micro-segmentation may be implemented within the underlying service provider's infrastructure).

SC-7(3): Limit the number of external network connections to the system to only those essential for business or mission operations. All system and device management interfaces must not be exposed to the public internet.

SC-7(4): In addition to the standards above, implement the following boundary protection enhancements:

- Implement a managed interface for each external telecommunication service;
- Establish a traffic flow policy for each managed interface;
- Protect all externally facing web applications and services using a Web Application Firewall (WAF);
- Management interfaces are prohibited from being accessible from the internet;
- Protect the confidentiality and integrity of the information being transmitted across each interface;
- Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;
- Review exceptions to the traffic flow policy quarterly and remove exceptions that are no longer supported by an explicit mission or business need;
- Prevent unauthorized exchange of control plane traffic with external networks;
- Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and
- Filter unauthorized control plane traffic from external networks.

SC-7(5): Deny network communications traffic by default and allow network communications traffic by exception (e.g., deny all, permit by exception) at all managed interfaces.

SC-7(7): Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is explicitly authorized by the agency's Authorizing Official (AO), and uses authorized secure remote access technologies (e.g., such as VPN, Zero Trust Network Access (ZTNA), SASE) with controlled routing policies, encryption and authentication for both tunneled and split traffic, and hardened and monitored endpoints.

SC-7(8): Route IT traffic to external networks through authenticated proxy servers at managed interfaces.

318-6 Protect Transmitted Information (SC-8)

Protect the confidentiality of transmitted information. Plan for cryptographic agility, including documented transition strategies for deprecated or weakened cryptographic algorithms.

Post Quantum Cryptography

As quantum computing advances, traditional cryptographic algorithms face obsolescence. These algorithms rely on mathematical problems that quantum computers can solve exponentially faster than classical machines, posing a significant threat to data confidentiality, integrity, and trust. Post Quantum Cryptography (PQC) methods are designed to resist attacks from both classical and quantum computers. Unlike quantum cryptography, which requires specialized hardware, PQC is software-based and deployable on existing infrastructure, making it a practical and scalable solution for public and private sector organizations.

SC-8(1): Implement cryptographic mechanisms to prevent unauthorized disclosure of information during transmission. Agencies shall utilize encryption standards that align with current guidance from the NIST, with preference given to those designed to resist emerging post-quantum threats. Where Federal Information Processing Standards (FIPS)-140 validation is explicitly required by data protection regulations (e.g., Federal personally identifiable information (PII), Criminal Justice Information Services (CJIS), Federal Risk and Authorization Management Program (FedRAMP), Cybersecurity Maturity Model Certification (CMMC) , Gramm-Leach-Bliley Act (GLBA)), the level of FIPS validation is defined by the regulatory body.

Encryption Standards

Cryptographic Use	NIST Reference*
Post-Quantum Algorithms	NIST SP 1800-38 - Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography
Cryptographic Algorithms and Key Lengths	NIST SP 800-131A - Transitioning the Use of Cryptographic Algorithms and Key Lengths
Symmetric / Asymmetric Encryption	NIST SP 800-175B - Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms

Cryptographic Use	NIST Reference*
Hash Functions	NIST 800-107 - Recommendation for Applications Using Approved Hash Algorithms
Digital Signatures	FIPS 186-5 - Digital Signature Standard (DSS)
Key Establishment	NIST SP 800-56A - Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography
TLS Protocols	NIST SP 800-52 - Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations

**Revisions may change, utilize latest revision published by NIST.*

Where FIPS-140 validation is explicitly required by data protection regulations (e.g., Federal PII, CJIS, FedRAMP, CMMC, GLBA) the level of FIPS validation is defined by the regulatory body.

318-7 Terminate Network Connections (SC-10)

Terminate the network connection associated with a communications session at the end of the session or 30 minutes of inactivity.

318-8 Cryptographic Key Establishment and Management (SC-12)

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements:

- Establishing manual procedures or automated mechanisms for digital certificate generation, installation, and distribution;
- Generating and storing subscriber key pairs using a minimum key length of 128-bit encryption; and where feasible, FIPS 140-2 (or its successor);
- Prohibiting the use of the same public/private key pairs for encryption and digital signatures;
- Protecting private keys using strong, complex passwords, which are in line with DoIT's Password policy; and
- Revoking certificates if the associated private key is compromised, revocation is requested by management, or the certificate is no longer needed.

Note: Additional guidance is provided in NIST SP 800 133, Recommendation for Cryptographic Key Generation.

318-9 Implement Cryptographic Protection (SC-13)

Implement FIPS 140-3 (or existing FIPS 140-2 validated modules until their retirement on September 21, 2026) compliant cryptographic modules for non-public, regulated information (e.g., PII, Health Insurance Portability and Accountability Act (HIPAA), Federal Tax Information (FTI)).

318-10 Restrict Collaborative Computing Devices and Applications (SC-15)

Prohibit remote activation of collaborative computing devices and applications (e.g., including networked white boards, cameras, and microphones) with any exceptions documented; and Provide an explicit indication of use to users physically present at the devices (i.e., signals to users when collaborative computing devices are activated).

318-11 Issue Public Key Infrastructure Certificates (SC-17)

Where Public Key Infrastructure (PKI) management is not handled by a service provider, the agency shall issue public key certificates under an internal Certificate Authority (CA) that governs the operation of the PKI or obtain public key certificates from a trusted CA or a designated third-party provide; and include only approved trust anchors in trust stores or certificate stores managed by the organization.

Common Uses of PKI Certificates

Technology Types	Certificate Descriptions
Web Servers & Applications	TLS/ (Secure Sockets Layer (SSL) certificates for secure Hypertext Transfer Protocol Secure (HTTPS) connections
Email Systems	Certificates for encrypted and signed email
VPN/Remote Access	User/device authentication using PKI certificate
Endpoint Security	Device/user authentication via certificate-based login
Digital Signatures	FIPS 186-5 - Digital Signature Standard (DSS)
Cloud Platforms	Manage trust anchors and certificate issuance
Mobile Device Management (MDM)	Device certificates for compliance
Identification & Authentication	Issue and validate certificates for user access control
Code Signing & Software Integrity	Ensure authenticity and integrity of software packages

318-12 Control the Use of Mobile Code (SC-18)

Define acceptable and unacceptable mobile code and mobile code technologies; and authorize, monitor, and control the use of mobile code within the system. Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, and VBScript.

Note: For specific details on the mobile code standards and guidelines, see *NIST SP 800-28 Guidelines on Active Content and Mobile Code*.

318-13 Employ Secure Name/Address Resolution Service (Authoritative Source) (SC-20)

Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

318-14 Employ Secure Name/Address Resolution Service (Recursive or Caching Resolver) (SC-21)

Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

For specific details on secure Domain Name System (DNS) deployment, see *NIST SP 800-81-2 Secure Domain Name System (DNS) Deployment Guide.*

318-15 Employ Architecture and Provisioning for Name/Address Resolution Service (SC-22)

Validate systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.

318-16 Protect Session Authenticity (SC-23)

Protect the authenticity of communications sessions using risk-based and context-aware safeguards. This control addresses communications protection at the session, versus packet level, and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted.

Context-Aware Safeguards

Session protection refers to the set of mechanisms that ensure a user's authenticated session remains valid, secure, and resistant to hijacking or misuse. Session hijacking and token theft remain persistent threats in hybrid environments. Strengthening session integrity ensures that authenticated users remain verified throughout their interaction lifecycle. Context aware validation evaluates additional environmental and behavioral signals beyond just credentials before granting or maintaining access and is a cornerstone of modern ZTA and adaptive access control.

Common Authenticity Protections

Protection Types	Description
Internet Protocol (IP) Address Binding	Require re-authentication if the session token is used from a different IP address than the one it was issued from. This helps detect lateral movement or token replay from unauthorized locations
User-Agent (UA) String Validation	Monitor for changes in browser or device fingerprints. A mismatch in UA strings can indicate session theft or automated scraping attempts.
Session Rotation on Privilege Escalation	Automatically rotate session tokens when a user elevates privileges (e.g., from viewer to admin) to prevent privilege abuse from stale tokens.
Idle Timeout + Absolute Expiry	Enforce short idle timeouts and hard session expiration windows to reduce exposure from abandoned or long-lived sessions.
Geo-Velocity Checks	Flag or invalidate sessions if the same token is used from geographically distant locations within a short time frame.
Cookie Attributes	Use HttpOnly, Secure, and SameSite=Strict flags to prevent client-side access and cross-site request forgery.

318-17 Protect of Information at Rest (SC-28)

At a minimum, protect the confidentiality and integrity of information at rest with:

- Configuration of rule sets for firewalls, gateway, intrusion detection/prevention systems, filtering routers, authenticator information;
- Cryptographic mechanisms, row-level and column-level security, database activity monitoring, and audit logging for all databases maintaining non-public State data; and
- Security controls for all backup media and replicated data stores, including encryption at rest, strict access controls, integrity validation, and protection against unauthorized replication, modification, or restoration.

SC-28(1): Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of information at rest on any State asset that stores regulated information (e.g., PII, HIPAA, FTI) .

Layered Encryption for Systemwide Resilience

Encryption has to be applied at every layer of a system because each layer protects a different exposure point, and no single mechanism can defend the entire data lifecycle. Network-level encryption shields data as it moves between components, but once it reaches the database, only database-specific controls like column-level encryption and encrypted backups can prevent disclosure through stolen media, compromised storage, or unauthorized access to archived data. Application-level encryption ensures that even if the database or infrastructure is breached, the most sensitive fields remain unreadable without the application's keys. Storage-level encryption adds another boundary by protecting disks, snapshots, and cloud volumes from offline attacks, while key-management layers ensure that all these protections remain trustworthy by securing the cryptographic material itself.

318-18 Process Isolation (SC-39)

Maintain a separate execution domain for each executing system process. Every program or task that runs on a system should operate in its own isolated environment. This helps prevent one process from interfering with or accessing another, especially if something goes wrong or gets compromised.

Information systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each information system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. This capability is available in most commercial operating systems that employ multi-state processor technologies.

GUIDELINES

ID	Title	Description	Source
CSF Tools	Cyber Security Framework Tools	This website provides supplemental guidance for each security control listed in this document.	*csf.tools (LINK)*
NIST SP 800-215	Guide to a Secure Enterprise Network Landscape	This document provides security guidance for modern enterprise networks, addressing challenges such as cloud access, micro-services-based applications, and geographically distributed IT resources.	*csf.tools (LINK)*
NIST SP 800-88	Guidelines for Media Sanitization	This document provides best practices for securely disposing of data stored on various types of media to prevent unauthorized access or data recovery.	*csf.tools (LINK)*
NIST SP 131A	Transitioning the Use of Cryptographic Algorithms and Key Lengths	Guide for transitioning to stronger cryptographic algorithms and key lengths across federal systems.	*csf.tools (LINK)*
NIST SP 800-133	Recommendation for Cryptographic Key Generation	This document provides guidance on secure key generation methods for approved cryptographic algorithms.	*csf.tools (LINK)*
NIST SP 800-57 Part 1	Recommendation for Key Management	This document provides background information support appropriate decisions when selecting and using cryptographic mechanisms.	*csf.tools (LINK)*
NIST SP 800-28	Guidelines on Active Content and Mobile Code	This document provides guidelines on active content and mobile code, focusing on security risks and mitigation strategies.	*csf.tools (LINK)*
DoD Reference	Department of Defense (DoD) Zero Trust Reference Architecture	This document is an example of how other organizations (i.e., Department of Defense) approach cybersecurity being updated to become data centric and infuse ZT principles.	*DoD: (LINK)*
NIST SP-800-81-2	Secure Domain Name System (DNS) Deployment Guide	This document provides guidelines for implementation strategies like DNSSEC	*csf.tools (LINK)*

DEFINITIONS

Each unique term used in this standard is defined in the **State of Maryland Cybersecurity & Privacy Glossary**.

COMPLIANCE CHECKLIST

ID	Standard	Compliance
318-1	**Develop Agency-Level Procedures (SC-1)**	☐ Yes ☐ No
318-2	**Separate System and User Functionality (SC-2)**	☐ Yes ☐ No
318-3	**Protect Shared System Resources (SC-4)**	☐ Yes ☐ No
318-4	**Protect Against Denial-of-Service (SC-5)**	☐ Yes ☐ No
318-5	**Implement Boundary Protection (SC-7)**	☐ Yes ☐ No
318-6	**Protect Transmitted Information (SC-8)**	☐ Yes ☐ No
318-7	**Terminate Network Connections (SC-10)**	☐ Yes ☐ No
318-8	**Cryptographic Key Establishment and Management (SC-12)**	☐ Yes ☐ No
318-9	**Implement Cryptographic Protection (SC-13)**	☐ Yes ☐ No
318-10	**Restrict Collaborative Computing Devices and Applications (SC-15)**	☐ Yes ☐ No
318-11	**Issue Public Key Infrastructure Certificates (SC-17)**	☐ Yes ☐ No
318-12	**Control the Use of Mobile Code (SC-18)**	☐ Yes ☐ No
318-13	**Employ Secure Name/address Resolution Service (authoritative Source) (SC-20)**	☐ Yes ☐ No
318-14	**Employ Secure Name/address Resolution Service (recursive or Caching Resolver) (SC-21)**	☐ Yes ☐ No
318-15	**Employ Architecture and Provisioning for Name/address Resolution Service (SC-22)**	☐ Yes ☐ No
318-16	**Protect Session Authenticity (SC-23)**	☐ Yes ☐ No
318-17	**Protect of Information at Rest (SC-28)**	☐ Yes ☐ No
318-18	**Process Isolation (SC-39)**	☐ Yes ☐ No

Note: When assessing the implementation and effectiveness of the security and privacy controls outlined in this standard, DoIT recommends the use of NIST SP 800-53A Rev. 5, to perform evaluations in a manner that is evidence-based, repeatable, and aligned with the system's documented security posture.