State of Maryland

STANDARD

PROGRAM MANAGEMENT

Document No.	Last Updated	Prepared By
MD-STD-313-PM-01	02/18/2026	DOIT OSM

Program management provides the foundational governance structure that supports the State's overall security posture. Unlike system-specific controls, Program Management standards operate at the enterprise level, guiding how security policies, risk strategies, and resource planning are developed, implemented, and maintained across all agencies and systems.

PURPOSE AND SCOPE

Purpose	This standard provides the technical and operational specifications needed to oversee and coordinate cybersecurity programs.
Scope	This standard is designed to help agencies implement and oversee cybersecurity and privacy programs at a strategic level.
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. **This standard provides agencies with insight into enterprise-level initiatives, and the standards used to guide those initiatives.**
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.

FOREWORD

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

313 State Strategy

These standards establish State-wide governance and strategic oversight, including risk management, capital planning, and continuous monitoring. **This standard also provides agencies with visibility into enterprise-level initiatives.**

313-1 Develop Agency-Level Procedures (PM-1)

The DoIT Office of Security Management (OSM) will develop and disseminate a Maryland Cybersecurity & Privacy Policy Suite to agencies in support of their agency-level program management activities. Agencies must disseminate the policies and standards to agency personnel with information technology (IT) security responsibilities for awareness and alignment in agency-level procedures.

Related Policy & Standards:
MD-POL-100 Cybersecurity & Privacy Governance Policy

313-2 Establish an Information Security Program Leadership Role (PM-2)

OSM will assign Information Security Officers (ISOs) to provide agencies with security expertise, guidance, and resources to assist agencies in meeting State and Federal cybersecurity compliance requirements. Where feasible, agencies are encouraged to appoint a senior agency Authorizing Official (AO), or similar security oversight role, with the mission and resources to coordinate with the State Chief Information Security Officer (SCISO), State Chief Privacy Officer (SCPO) and State Chief Data Officer (SCDO) on security, privacy, and data governance initiatives.

Related Policy & Standards:
MD-POL-100 Cybersecurity & Privacy Governance Policy
MD-POL-201 Cybersecurity Risk Management Policy
MD-STD-304 Control Assessments Standard

313-3 Allocate Information Security and Privacy Resources (PM-3)

OSM will include the resources needed for DoIT to implement the enterprise information security and privacy programs in capital planning and investment requests. DoIT will prepare documentation required for addressing information security and privacy programs in capital planning and investment requests. Agencies are encouraged to include cybersecurity and privacy policy compliance as a line item in agency budgets.

Related Policy & Standards:
MD-POL-100 Cybersecurity & Privacy Governance Policy
MD-POL-201 Cybersecurity Risk Management Policy
MD-STD-317-SA System & Services Acquisition Standard

313-4 Maintain a Plan of Action and Milestones Process (PM-4)

OSM will create and maintain a plan of action and milestones (POA&M) for the development and operationalization of enterprise information security, privacy, and supply chain risk management (SCRM) enterprise programs. DoIT will review plans of action and milestones for consistency with the Enterprise Risk Management (ERM) strategy and State-wide priorities for risk response actions.

Related Policy & Standards:
MD-POL-100 Cybersecurity & Privacy Governance Policy
MD-POL-201 Cybersecurity Risk Management Policy

313-5 Maintain a System Inventory (PM-5)

Agencies shall develop and maintain an inventory of their information systems and provide OSM with visibility into this inventory to support enterprise-wide oversight and risk management.

PM-5(1): The SCPO will guide agencies in the completion of privacy threshold analysis (PTA) to identify all systems, applications, and projects that process personally identifiable information.

Related Policy & Standards:
MD-POL-202 Asset Management Policy
MD-STD-305-CM Configuration Management Standard

313-6 Measure Security and Privacy Performance (PM-6)

OSM will guide agencies on best practices for information security and privacy measures of performance. Agencies are encouraged to develop, monitor, and report on the results of information security and privacy performance metrics.

Related Policy & Standards:
MD-POL-100 Cybersecurity & Privacy Governance Policy

313-7 Maintain an Enterprise Architecture (PM-7)

OSM and DoIT will contribute subject matter expertise to the development and maintenance of the DoIT Enterprise Architecture (EA) integrating Zero Trust Architecture (ZTA) principles, information security, privacy, and the risk to agency operations and assets, individuals, and the State.

PM-7(1): Agencies may consider offloading non-essential functions or services to other systems, system components, or an external provider when doing so reduces the attack surface, minimizes resource exposure, or enforces least privilege principles.

Related Policy & Standards:
MD-STD-312-PL Planning Standard

313-8 Develop a Critical Infrastructure Plan (PM-8)

OSM will address information security and privacy issues related to the development, documentation, and updating of a critical infrastructure and key resources.

Related Policy & Standards:
MD-POL-201 Cybersecurity Risk Management Policy
MD-POL-210 Continuity of Operations Policy
MD-STD-306-CP Contingency Planning Standard
MD-STD-311-PE Physical & Environmental Protection Standard

313-9 Develop a Risk Management Strategy (PM-9)

The Governance Risk and Compliance (GRC) Team within OSM will develop a comprehensive strategy for managing the risk to the State's information technology assets.

Related Policy & Standards:
MD-POL-201 Cybersecurity Risk Management Policy
MD-STD-304-CA Control Assessments
MD-STD-316-RA Risk Assessment Standard

313-10 Develop an Authorization Process (PM-10)

The GRC Team is responsible for the State's Authorization to Operate (ATO) Process. DoIT ISOs will guide agencies in the management of security and privacy of agency systems and the environments in which those systems operate using the State ATO Process. Agencies will be required to designate individuals to fulfill specific roles and responsibilities within the agency to operationalize the risk management process.

Related Policy & Standards:
MD-POL-201 Cybersecurity Risk Management Policy
MD-STD-304-CA-01 Control Assessments
MD-STD-316-RA Risk Assessment Standard

313-11 Define Mission and Business Processes (PM-11)

Agencies should define mission and business processes with consideration for information security and privacy and the resulting risk to agency operations, agency assets, individuals, other organizations, and the State. The SCISO and SCPO will guide agencies in the determination of information protection and PII processing needs arising from the defined mission and business processes. When PII is processed, agencies will be required to update the Privacy Impact Assessment accordingly and review and revise the mission and business processes annually.

Related Policy & Standards:
MD-STD-312-PL Planning Standard
MD-STD-317-SA System & Services Acquisition Standard

313-12 Implement an Insider Threat Program (PM-12)

DoIT will guide agencies on best practices for implementing an insider threat program, including guidelines for handling insider threat events.

Related Policy & Standards:
MD-STD-301-AC Access Control Standard
MD-STD-303-AU Audit & Accountability
MD-STD-314-PS Personnel Security Standard
MD-STD-316-RA Risk Assessment Standard

313-13 Develop Security and Privacy Workforce (PM-13)

OSM will guide agencies on available resources for security and privacy workforce development and improvement.

Related Policy & Standards:
MD-POL-206 Awareness & Training Policy
MD-STD-302-AT Awareness & Training Standard

313-14 Conduct Testing, Training, and Monitoring (PM-14)

OSM will guide agencies, as part of the State risk management strategy, on methods for conducting security and privacy testing, training, and monitoring activities associated with agency systems.

Related Policy & Standards:
MD-POL-208 Continuous Monitoring Policy
MD-STD-304-CA Control Assessments

313-15 Affiliate with Security and Privacy Groups and Associations (PM-15)

Agencies are encouraged to establish and institutionalize contact with DoIT to:

- Facilitate ongoing security and privacy education and training for agency personnel;
- Maintain currency with recommended security and privacy practices, techniques, and technologies; and
- Share current security and privacy information, including threats, vulnerabilities, and incidents.

Agencies may engage DoIT and the MCCC when they need enterprise-level coordination, policy alignment, or cross-agency decision-making. Agencies may leverage MD-ISAC for operational threat intelligence, real-time alerts, and situational awareness.

Related Policy & Standards:
MD-STD-301-AC Access Control Standard

313-16 Implement a Threat Awareness Program (PM-16)

OSM has implemented the MD-ISAC as a threat awareness program that promotes cross-agency information-sharing for threat intelligence.

PM-16(1): MD-ISAC automates threat sharing to maximize the effectiveness of sharing threat intelligence information.

Related Policy & Standards:
MD-POL-208 Continuous Monitoring Policy
MD-STD-304-CA Control Assessments
MD-STD-319-SI System & Information Integrity Standard

313-17 Protect Controlled Unclassified Information on External Systems (PM-17)

Controlled Unclassified Information (CUI) is a federal designation established by Executive Order 13556 to standardize how the federal government handles sensitive but unclassified information across agencies and with external partners like the State of Maryland and its agencies.

The MD Cybersecurity & Privacy Policy Suite guides the protection of State data. This policy suite, which is explicitly aligned with the NIST SP 800-53 Rev. 5 control framework, implements a similar baseline security and privacy controls prescribed for federal systems. Agencies should review their alignment with the State policy suite and any CUI specific control requirements prior to the receipt of CUI in State systems.

Related Policy & Standards:
MD-POL-100 Cybersecurity & Privacy Governance Policy
MD-POL-205 Data Protection & Privacy Policy

313-18 Develop a Privacy Program Plan (PM-18)

The SCPO will develop a privacy program plan including best practices such as:

- A description of the structure of the privacy program and the resources dedicated to the privacy program;
- An overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements;
- The role of the senior agency official for privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities;
- Management commitment, compliance, and the strategic goals and objectives of the privacy program; and
- Coordination among State and agency entities responsible for the different aspects of privacy.

The plan will be updated as needed to address changes in privacy laws, policy and State changes, and problems identified during plan implementation or privacy control assessments.

Related Policy & Standards:
MD-POL-205 Data Protection & Privacy Policy
MD-STD-315-PT PII and Transparency Standard

313-19 Establish a Privacy Program Leadership Role (PM-19)

Agencies shall appoint a senior agency official for privacy with the authority, mission, accountability, and resources to coordinate, develop, and implement applicable privacy requirements and manage privacy risks in collaboration with the SCPO through the State-wide privacy program.

Related Policy & Standards:
MD-POL-100 Cybersecurity & Privacy Governance Policy
MD-POL-201 Cybersecurity Risk Management Policy
MD-STD-304 Control Assessments Standard

313-20 Disseminate Privacy Program Information (PM-20)

The SCPO will maintain a central source of information about the State's privacy program that:

- Provides the public with access to information about State privacy activities;
- Makes publicly available the State privacy practices and reports; and
- Employs publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or ask direct questions to privacy offices regarding privacy practices.

PM-20(1): OSM will develop and post cybersecurity and privacy policies on external-facing websites, mobile applications, or other digital services deemed most appropriate by OSM, that:

- Are written in plain language and organized in a way that is easy to understand and navigate;
- Provide information needed by the public to make an informed decision about whether and how to interact with the State; and
- Are updated whenever the State makes a substantive change to the practices it describes and includes a time/date stamp to inform the public of the date of the most recent changes.

Related Policy & Standards:
MD-POL-100 Cybersecurity & Privacy Governance Policy
MD-STD-315-PT PII and Transparency Standard

313-21 Maintain Accounting of Disclosures (PM-21)

The SCPO will guide agencies on developing and maintaining an accurate accounting of disclosures of PII, including date, nature, and purpose of each disclosure; and name and address, or other contact information of the individual or agency to which the disclosure was made.

Where required, agencies should retain the accounting of disclosures for the length of the time the PII is maintained or five years after the disclosure is made, whichever is longer; and make the accounting of disclosures available to the individual to whom the PII relates upon request.

Related Policy & Standards:
MD-POL-205 Data Protection & Privacy Policy

313-22 Manage the Quality of Personally Identifiable Information (PM-22)

The SCPO will guide agencies on:

- Reviewing for the accuracy, relevance, timeliness, and completeness of PII across the information life cycle;
- Correcting or deleting inaccurate or outdated PII;
- Disseminating notice of corrected or deleted PII to individuals or other appropriate entities; and
- Appealing adverse decisions on correction or deletion requests.

313-23 Establish a Data Governance Body (PM-23)

The Office of Enterprise Data (OED) will establish a Data Governance Body consisting of SCDO-defined roles and responsibilities.

Related Policy & Standards:
MD-POL-205 Data Protection & Privacy Policy

313-24 Establish a Data Integrity Board (PM-24)

The SCPO will establish a Data Integrity Board to review proposals to conduct or participate in a matching program; and conduct an annual review of all matching programs in which an agency has participated.

Related Policy & Standards:
MD-POL-205 Data Protection & Privacy Policy

313-25 Minimize Personally Identifiable Information Used in Testing, Training, and Research (PM-25)

The SCISO and SCPO will only authorize the use of PII for internal purposes when such information is required for internal testing, training, and research.

Related Policy & Standards:
MD-POL-205 Data Protection & Privacy Policy

313-26 Implement Complaint Management Process (PM-26)

The SCPO will implement a process for receiving and responding to complaints, concerns, or questions from individuals about the State security and privacy practices that includes:

- Mechanisms that are easy to use and readily accessible by the public;
- All information necessary for successfully filing complaints;
- Tracking mechanisms to review and address all complaints received within the allowable timeframe;
- Acknowledgement of receipt of complaints, concerns, or questions from individuals within the allowable timeframe; and
- Response to complaints, concerns, or questions from individuals within the timeframe advertised.

Related Policy & Standards:
MD-STD-315-PT PII and Transparency Standard

313-27 Conduct Privacy Reporting (PM-27)

Agencies will be required to develop SCPO-defined privacy reports and disseminate them to:

- SCPO-defined officials to demonstrate accountability with statutory, regulatory, and policy privacy mandates; and
- SCPO-defined officials with responsibility for monitoring privacy program compliance.

Agencies will review and update privacy reports annually or as directed by the SCPO.

Related Policy & Standards:
MD-POL-205 Data Protection & Privacy Policy
MD-STD-315-PT PII and Transparency Standard

313-28 Conduct Risk Framing (PM-28)

As part of the ERM, the SCISO, in collaboration with the SCPO and SCDO, will define:

- Assumptions affecting risk assessments, risk responses, and risk monitoring;
- Constraints affecting risk assessments, risk responses, and risk monitoring;
- Priorities and trade-offs considered by the State for managing risk; and
- Enterprise risk tolerance.

313-29 Establish Risk Management Program Leadership Roles (PM-29)

OSM will establish a Risk Executive function to view and analyze risk from a State-wide perspective. Where feasible, agencies are encouraged to appoint an agency-level CISO or Senior Accountable Official for Risk Management to align State information security and privacy management processes with strategic, operational, and budgetary planning processes.

Related Policy & Standards:
MD-POL-100 Cybersecurity & Privacy Governance Policy
MD-POL-201 Cybersecurity Risk Management Policy
MD-STD-304 Control Assessments Standard

313-30 Develop a Supply Chain Risk Management Strategy (PM-30)

OSM will guide agencies on managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services. Agencies should implement supply chain risk management activities consistently across the agency.

PM-30(1): Each agency should identify, prioritize, and assess suppliers of critical or mission-essential technologies, products, and services.

Related Policy & Standards:
MD-POL-201 Cybersecurity Risk Management Policy
MD-STD-320-SR Supply Chain & Risk Management Standard

313-31 Develop a Continuous Monitoring Strategy (PM-31)

OSM will develop a State-wide continuous monitoring strategy and implement continuous monitoring activities that includes:

- Establishing the CISO-defined metrics to be monitored;
- Establishing CISO-defined frequencies for monitoring and for assessment of control effectiveness;

- Ongoing monitoring of CISO-defined metrics in accordance with the continuous monitoring strategy;
- Correlation and analysis of information generated by control assessments and monitoring;
- Response actions to address results of the analysis of control assessment and monitoring information; and
- Reporting the security and privacy status of agency systems to SCISO, SCPO and SCDO as requested.

Related Policy & Standards:
MD-POL-208 Continuous Monitoring Policy
MD-STD-304-CA Control Assessments Standard
MD-STD-316-RA Risk Assessment Standard

313-32 Analyze System Purposing (PM-32)

Analyze agency systems or systems components that support mission-essential services or functions and implement technical and administrative controls to restrict information resources to their intended purposes in accordance with the principle of least functionality.

Related Policy & Standards:
MD-POL-201 Cybersecurity Risk Management Policy

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 800-39	Managing Information Security Risk: Organization, Mission, and Information System View	This guideline focuses on managing information security risk at an organization-wide level. It provides a structured approach to risk management that integrates security into mission, business processes, and system operations.	*csrc.nist.gov (LINK)*
NIST Privacy Framework	NIST Privacy Framework	This is a voluntary tool designed to help organizations manage privacy risks while enabling innovation. It provides structured guidance for identifying, assessing, and mitigating privacy concerns within an enterprise risk management approach.	*csrc.nist.gov (LINK)*

DEFINITIONS

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

COMPLIANCE CHECKLIST

ID	Standard	Compliance
313-1	Develop Agency-Level Procedures (PM-1)	☐ Yes ☐ No
313-2	Establish an Information Security Program Leadership Role (PM-2)	☐ Yes ☐ No
313-3	Allocate Information Security and Privacy Resources (PM-3)	☐ Yes ☐ No
313-4	Maintain a Plan of Action and Milestones Process (PM-4)	☐ Yes ☐ No
313-5	Maintain a System Inventory (PM-5)	☐ Yes ☐ No
313-6	Measure Security and Privacy Performance (PM-6)	☐ Yes ☐ No
313-7	Maintain an Enterprise Architecture (PM-7)	☐ Yes ☐ No
313-8	Develop a Critical Infrastructure Plan (PM-8)	☐ Yes ☐ No
313-9	Develop a Risk Management Strategy (PM-9)	☐ Yes ☐ No
313-10	Develop an Authorization Process (PM-10)	☐ Yes ☐ No
313-11	Define Mission and Business Processes (PM-11)	☐ Yes ☐ No
313-12	Implement an Insider Threat Program (PM-12)	☐ Yes ☐ No
313-13	Develop Security and Privacy Workforce (PM-13)	☐ Yes ☐ No
313-14	Conduct Testing, Training, and Monitoring (PM-14)	☐ Yes ☐ No
313-15	Affiliate with Security and Privacy Groups and Associations (PM-15)	☐ Yes ☐ No
313-16	Implement a Threat Awareness Program (PM-16)	☐ Yes ☐ No
313-17	Protect Controlled Unclassified Information on External Systems (PM-17)	☐ Yes ☐ No
313-18	Develop a Privacy Program Plan (PM-18)	☐ Yes ☐ No
313-19	Establish a Privacy Program Leadership Role (PM-19)	☐ Yes ☐ No
313-20	Disseminate Privacy Program Information (PM-20)	☐ Yes ☐ No
313-21	Maintain Accounting of Disclosures (PM-21)	☐ Yes ☐ No

313-22	**Manage the Quality of Personally Identifiable Information (PM-22)**	☐ Yes ☐ No
313-23	**Establish a Data Governance Body (PM-23)**	☐ Yes ☐ No
313-24	**Establish a Data Integrity Board (PM-24)**	☐ Yes ☐ No
313-25	**Minimize Personally Identifiable Information Used in Testing, Training, and Research (PM-25)**	☐ Yes ☐ No
313-26	**Implement Complaint Management Process (PM-26)**	☐ Yes ☐ No
313-27	**Conduct Privacy Reporting (PM-27)**	☐ Yes ☐ No
313-28	**Conduct Risk Framing (PM-28)**	☐ Yes ☐ No
313-29	**Establish Risk Management Program Leadership Roles (PM-29)**	☐ Yes ☐ No
313-30	**Develop a Supply Chain Risk Management Strategy (PM-30)**	☐ Yes ☐ No
313-31	**Develop a Continuous Monitoring Strategy (PM-31)**	☐ Yes ☐ No
313-32	**Analyze System Purposing (PM-32)**	☐ 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.