STATE OF MARYLAND INFORMATION TECHNOLOGY SECURITY MANUAL

Version 1.2

June 28, 2019

Table of Contents

RECORD OF REVISIONS

Version	Date	Description
Version 0.2	10/21/2018	Added all security controls tables and updated text to reflect current requirements, guidelines and best practices.
Version 0.3	11/14/2018	Initial round of revisions made from DoIT Executive review.
Version 0.4	03/15/2019	All revisions from legal review made

Purpose

The purpose of the Maryland IT Security Manual is to describe the security requirements with which executive departments and independent state agencies must comply to protect the confidentiality, integrity and availability of Maryland Information Systems (MIS) and State-owned data. This document serves as the primary policy for establishing and defining the State's mandated IT security practices and requirements for all Maryland agencies.

The IT security policies captured within this Manual were developed to align with federal and state government standards and procedures issued by the National Institute of Standards and Technology (NIST), the Centers for Medicare and Medicaid Services (CMS), Internal Revenue Service (IRS), Office of Legislative Audits (OLA), Office of Management and Budget (OMB), and the General Services Administration (GSA).

It is noted that Maryland Agencies may set their own organizational policies, based on its individual business needs or specific legal requirements such as the Health Insurance Portability and Accountability Act (HIPAA), which may exceed the security requirements expressed in this Manual, but must, at a minimum, conform to the minimum requirements.

Scope

The policy applies to any MIS that electronically generates, receives, stores, processes or transmits State-owned data, whether the system is hosted on the state network or by a third-party provider. Additionally, the provisions of this Manual apply to all Maryland state employees, contractors, and potential information system users (both internal and external). This policy is developed and owned by the Maryland Department of Information Technology (DoIT).

Update and Review

This policy must be reviewed, at a minimum, on an annual basis and updated when necessary. Policy reviews/updates may be performed more frequently because of environmental or legal changes (e.g., changes in federal or state mandates, privacy requirements, etc.).

Authority

The Maryland Department of Information Technology (DoIT) has the authority to set policy and provide guidance and oversight for the security and privacy of all the IT systems in accordance with Maryland Code, State Finance and Procurement § 3A-303 and § 3A-305. In addition, the most critical federal and state laws, regulations, executive orders, policies, standards, and directives followed are indicated below:

- Clinger-Cohen Act of 1996
- CMS Information Systems Security and Privacy Policy (IS2P2)
- E-Government Act of 2002

- Federal Acquisition Streamlining Act of 1994 (FAFSA)
- Federal Financial Management Improvement Act of 1996 (FFMIA)
- Federal Information Processing Standards (FIPS)
- Federal Information Security Modernization Act of 2002, 2014 (FISMA)
- General Services Administration (GSA)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- IRS Publication 1075 - Tax Information Security Guidelines For Federal, State, and Local Agencies
- Manual (FISCAM)
- Maryland Executive Order 01.01.2017.22
- National Technology Transfer and Advancement Act of 1996
- NIST Special Publications
- Office of Legislative Audits (OLA)
- OMB Circulars
- OMB Memoranda
- Privacy Act of 1974

Preface

Information and information technology (IT) systems are essential assets of the State and vital resources to Maryland citizens. These assets are critical to the services that agencies provide to citizens, businesses, and educational institutions, as well as to local and federal government entities. All information created with State resources for State operations is the property of the State of Maryland. All agencies, employees, and contractors of the State are responsible for protecting such information from unauthorized access, modification, disclosure and destruction. This Policy sets forth a minimum level of security requirements that, when implemented, will provide the confidentiality, integrity and availability of Maryland IT Maryland Information Systems (MIS) and State-owned data.

The NIST is a non-regulatory federal agency within the US Department of Commerce. NIST's mission is to promote US innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

In general, the State of Maryland has adopted NIST information security related standards and guidelines. Security policies developed to secure an agency's information system should[1] refer to an NIST standard [and] agencies must develop procedures to ensure compliance with the policy. If there is no applicable published NIST standard or a published standard is deemed insufficient, agencies must adopt industry accepted security guidelines (or develop them) and refer to them within their security policy.

While state agencies are required to follow certain specific requirements in accordance with this policy, there is flexibility in how agencies apply NIST guidance. State agencies should apply the security concepts and principles articulated in the NIST Special Publications (SP) in accordance with and in the context of the agency's mission, business functions, and environment of operation. Consequently, the application of NIST guidance can result in different security solutions that are equally acceptable and compliant. When assessing state agency compliance with NIST SP, evaluators, auditors, and assessors should consider the intent of the security concepts within the specific guidance document and how the agency applied the guidance in the context of its mission/business responsibilities, operational environment, and unique organizational conditions.

Roles and Responsibilities

The following policy sets the minimum level of responsibility for the following individuals and groups:

[1] Use of the word "should" throughout this Manual should be interpreted to mean "shall" or "must," (e.g., establishing a requirement).

- Maryland Department of Information Technology;
- Maryland state agencies; and
- Employees and contractors.

Additionally, DoIT defines the following mandatory/key roles and responsibilities that must be assigned by each Maryland state agency:

- Authorizing Official;
- Chief Information Security Officer;
- System Owner; and
- Incident Response Team

If DoIT manages the IT Organization for the Maryland agency, then DoIT will assign the mandatory roles as required.

Department of Information Technology

- The duties of the Department of Information Technology are:
- Providing IT governance and oversight for all applicable Maryland state agencies;
- Developing, maintaining, and revising IT policies, procedures, and standards;
- Providing guidance, technical assistance, and recommendations to the Governor and units of the State Government concerning IT matters;
- Developing and maintaining a statewide IT master plan; and
- Adopting by regulation and enforcing non-visual access standards to be used in the procurement of IT services by or on behalf of units of the State Government.

Agency

Information security is an agency responsibility shared by all members of the Maryland state agency management team. The management team must provide clear direction and visible support for security initiatives. Each agency is responsible for:

- Initiating measures to assure and demonstrate compliance with the security requirements outlined in this policy;
- Implementing and maintaining an IT Security Program;
- Designating roles/responsibilities (defined in the *Roles and Responsibilities* section) to individuals for implementing and maintaining the agency security program;
- Ensuring that security is part of the information planning and procurement process;
- Participating in annual information systems data security self-audits focusing on compliance to this State data security policy;
- Determining the feasibility of conducting regular external and internal vulnerability assessments and penetration testing to verify security controls are working properly and to identify weaknesses;
- Archiving security assessment results for a minimum of (10) years and making them available to DoIT upon request;
- Implementing a risk management process for the life cycle of each critical IT

System;
- Assuring the confidentiality, integrity, availability, and accountability of all agency information while it is being processed, stored, or transmitted electronically, and the security of the resources associated with those processing functions;
- Assuming the lead role in resolving Agency security and privacy incidents in accordance with DoIT Incident Response procedures;
- Abiding by the guidelines established in Title 10, Subtitle 13 of the State Government Article “Protection of Information by Government Agencies;
- Developing, implementing and testing of an IT Disaster Recovery Plan for critical agency IT Systems in accordance with IT Disaster Recovery Plan Guidelines;
- Ensuring separation of duties and assigning appropriate system permissions and responsibilities for agency system users;
- Abiding by the Records Management Guidelines established by the Department of General Services and the Maryland State Archives; and
- Identifying “business owners” for any new system that are responsible for:
    - Classifying data;
    - Approving access and permissions to the data;
    - Ensuring methods are in place to prevent and monitor inappropriate access to confidential data; and
    - Determining when to retire or purge the data.

Employees and Contractors

All state employees and contract personnel are responsible for:

- Being aware of and complying with statewide and agency policies for the protection of IT assets;
- Using IT resources only for intended purposes as defined by policies, laws and regulations of the State or agency; and
- Being accountable for their actions relating to their use of all IT Systems.

Authorizing Official (AO)

The Authorizing Official (AO) formally assumes responsibility for operating the MIS at an acceptable level of risk to organizational operations, organizational assets, individuals, and other organizations. The following authorization decisions can be made by the AO:

- Authorization To Operate (ATO) – Full authorization may be granted when all of the following apply:
    - The authorization package is complete.
    - No corrective actions are required or only minor corrective actions are required. (Note: There may be findings during the authorization effort that are turned into a Plan of Action and Milestones (POA&M), but do not prevent an ATO).
    - Residual risks are acceptable to the AO.

- Authorization To Operate (ATO) with Conditions – Special type of authorization allowing an information system to operate in an operational environment by assessing a limited set of controls to include volatile controls as defined by NIST. This type of authorization will be given only when a system needs to be put in production to support continuity of organizational mission and business requirements. The system will be authorized to operate for a specified time in accordance with the terms and conditions established by the AO. This limited authorization will be granted when all of the following apply:
    - Vulnerability scans have been performed on the system and there are no major or high-risk vulnerabilities discovered. If necessary corrective actions (POA&Ms) are identified.
    - Volatile controls, as determined by the agency, have been assessed.
    - Residual risks are accepted for a limited time which is to be identified in the ATO letter, which also includes all terms and conditions needing to be satisfied.
- Interim Authority to Test (IATT) – The AO can exercise its authority to grant this special type of authorization allowing an information system to operate in an operational environment for the express purpose of testing the system with actual operational (e.g., live) data for a specified time. An IATT is granted by an AO only when the operational environment or live data is required to complete specific test objectives.
- Denial of Authorization to Operate (DATO) – If the AO, after reviewing the authorization package and any additional inputs provided by the risk executive (function), deems that the risk to organizational operations and assets, individuals, and other organizations, is unacceptable and immediate steps cannot be taken to reduce the risk to an acceptable level, a DATO is issued for the information system or for the common controls inherited by organizational information systems. The system may not be placed into operation until at least an IATT is granted.

Agency Chief Information Security Officer (CISO)

The CISO manages the Agency's IT Security and Risk Management Program.

The CISO has the following IT Security responsibilities:

- Develop, maintain, and oversee the Agency IT Security Program
- Monitor and report IT security program compliance with DoIT
- Serve as the IT security liaison to DoIT and external organizations
- Ensure sufficient resources are available to implement the Agency IT security program in coordination with the Agency business units
- Ensure, in coordination with senior Agency officials, the implementation of the

requirements of an Agency-wide IT Security Program (as specified in § 3544, paragraph (b), of the Federal Information Security Management Act (FISMA))

- Ensure that the Agency performs an independent evaluation of the IT Security Program and its practices, at minimum annually (as specified in § 3545 of the FISMA)
- Provide overall management and leadership and direction to the IT Security Program
- Assist and advise senior Agency officials regarding their responsibilities for security
- Report on the status of the IT Security Program to senior Agency officials and DoIT
- Consult with and brief Agency Executive Management regarding all critical information system security issues
- Ensure managers for all IT resources are identified and that security authorization for those resources are accomplished within the planned time-frame
- Determine the acceptable level of residual risk for an information subsystem and if an information subsystem will adequately protect sensitive information
- Review the MIS Security Authorization Package (SAP) and sign documents that require CISO signature
- Ensure Agency IT security planning and execution is practiced throughout the life cycle of each Agency MIS
- Ensure an Agency Incident Response Team (IRT) is staffed, trained, and maintained in a state of readiness
- Ensure that persons with IT security responsibilities have appropriate role-based training
- Assist oversight groups in compliance reviews and other reporting requirements
- Establish an overall strategy for the Agency IT Security Awareness and Training Program
- Ensure the program is sufficiently staffed and funded to achieve its approved objectives in a timely manner
- Ensure that Agency IT security policies are developed, approved and maintained in accordance with this Maryland IT Security Manual

System Owner (SO)

The System Owner (SO) has development and operational responsibility for the MIS. Multiple System Owners can be designated as required, however each MIS must have at least one (1) assigned SO. The SO has the following responsibilities for IT Security:

- Determine and implement an appropriate level of security commensurate with the system sensitivity level

- Categorize all information systems according to information type collected, maintained, used, stored, or processed by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels and in accordance with the System Security Categorization Policy, found in this document.
- Perform risk assessments (RA) annually or as part of continuous monitoring activities, to re-evaluate sensitivity of the system, risks, and mitigation strategies
- Take appropriate steps to reduce or eliminate vulnerabilities after receiving the results of continuous monitoring activities and update RAR accordingly
- Develop and maintain the MIS System Security Plan (SSP)
- Update the SSP during all continuous monitoring activities, including authorization, annual assessments and significant changes to the systems. During significant changes, where deemed necessary, the system should be reauthorized
- Establish system-level POA&M and implement and monitor corrective actions to timely completion
- Decide who has access to the system and grant individuals the fewest privileges necessary for job performance, re-evaluate the access privileges at least annually, and revoke access in accordance with DoIT guidelines upon personnel transfer, termination, or change in duties
- Ensure MIS personnel are properly designated, monitored, and trained, including appointment in writing of an individual to serve as the Technical Lead (TL), if appropriate
- Inform appropriate Agency officials of the need to conduct a security authorization effort and ensure that appropriate resources are available for the effort
- Assist in the identification, implementation, and assessment of security controls consistent with this Manual
- Ensure knowledge and skills to incorporate IT security throughout the system's Software Development Life Cycle (SDLC) process to protect the business operations and information the system supports
- Work with the CISO to meet shared IT security responsibilities

Incident Response Team (IRT)

The IRT serves as a single point of contact for security issues, coordinates incident response activities and performs assigned actions in accordance with this Manual which encompasses Continuous Monitoring, Situational Awareness, Event Management and Incident Handling. The IRT has the following additional IT Security responsibilities:

- Must ensure the Agency complies with specified Security Controls through operations standards contained in this Manual

- Takes appropriate action to alert appropriate personnel of suspected intrusions to the Agency MIS
- Analyze and document Information Security incidents and security events
- Perform investigations of potentially malicious or suspicious activity
- If the MIS stores, processes or transmits federal tax information, escalates or reports security incidents, as warranted, to the appropriate special agent-in-charge at the Treasury Inspector General for Tax Administration (TIGTA) and the IRS Office of Safeguards (Note: This applies only if the MIS stores, processes and/or transmits FTI data)
- Receive and monitor security alerts and advisories from US-CERT and take appropriate action in response to alerts and advisories
- Report security incident information to senior Agency officials and DoIT

Asset Management

All major information systems assets must be accounted for and have a named system owner. Accountability for assets helps to ensure that appropriate protection is maintained. System owners must be identified for all major assets and the responsibility for the maintenance of appropriate controls must be assigned. Responsibility for implementing controls may be delegated. Accountability must remain with the named business owner of the asset.

Inventory of Assets

Compiling an inventory of assets is an important aspect of risk management. Agencies need to be able to identify their assets and the relative values and importance of these assets. Based on this information, agencies can then provide appropriate levels of protection. Inventories of the important assets associated with each information system should be documented and maintained. Asset inventories must include; a unique system name, a system/business owner, a security classification and a description of the physical location of the asset. Examples of assets associated with information systems are:

- Information assets: databases and data files, system documentation, user manuals, training materials, operational or support procedures, disaster recovery plans, archived information;
- Software assets: application software, system software, development tools and utilities;
- Physical assets: computer equipment (processors, monitors, laptops, portable devices, tablets, smartphones, modems), communication equipment (routers, PBXs, fax machines, answering machines), magnetic media (tapes and disks), other technical equipment (uninterruptible power supplies, air conditioning units), furniture, accommodation; and

- Services: computing and communications services, general utilities (e.g., heating, lighting, power, air-conditioning).

Information Classification Policy

This section provides general requirements for data classification. The classification level definitions emphasize common sense steps to be taken to protect confidential information.

This policy pertains to all information within the State of Maryland systems that is processed, stored, or transmitted via any means. This includes: electronic information, information on paper, and information shared orally or visually. Data and record custodians must adhere to this policy and educate users that may have access to confidential information for which they are responsible.

All Maryland State information is categorized into two main classifications with regard to disclosure:

- Public
- Confidential

Public information is information that has been declared publicly available by Maryland State officials with the explicit authority to do so and can freely be given to anyone without concern for potential impact to the State of Maryland, its employees or citizens.

Confidential information is non-public information that has been deemed to constitute **Personally Identifiable Information (PII), Federal Tax Information (FTI), Protected Health Information (PHI), Payment Card Industry (PCI), Privileged or Sensitive, as defined below.**

Personally Identifiable Information (PII)

Personally Identifiable Information (PII). The term “PII,” as defined in State Government Art. 10-1301 as "an individual's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following data elements:

1) Social Security number;
2) Driver's license number, state identification card number, or other individual identification number issued by a unit;
3) Passport number or other identification number issued by the United States government;
4) Individual Taxpayer Identification Number; or
5) Financial or other account number, a credit card number, or a debit card number that, in combination with any required security code, access code, or password, would permit access to an individual's account.

Federal Tax Information (FTI)

FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS pursuant to an IRC 6103(p)(2)(B) Agreement.FTI includes any information created by the recipient that is derived from federal return or return information received from the IRS or obtained through a secondary source.

Protected Health Information (PHI)

PHI is health data created, received, stored, or transmitted by HIPAA-covered entities and their business associates in relation to the provision of healthcare, healthcare operations and payment for healthcare services. PHI includes all individually identifiable health information, including demographic data, medical histories, test results, insurance information, and other information used to identify a patient or provide healthcare services or health care coverage.

Payment Card Industry (PCI)

PCI pertains to personal data associated to an individual (cardholder) that uses credit, debit and/or cash cards for monetary transactions. PCI data includes account numbers, Social Security numbers, Date of Birth, and mailing addresses that associates a cardholder to a given payment account. Any information system that stores, processes, and/or transmits this data type must comply with the Payment Card Industry – Data Security Standard (PCI-DSS) control requirements to ensure cardholder data is appropriately protected from theft and fraudulent activities.

Privileged

Privileged records are protected from disclosure, which may include but is not limited to records:

- Relating to budgetary and fiscal analysis, policy papers, and recommendations made by the Department or by any person working for the Department;
- Provided by any other agency to the Department in the course of the Department's exercise of its responsibility to prepare and monitor the execution of the annual budget;
- Relating to State procurement when a final contract award has not been made or when disclosure of the record would adversely affect future procurement activity; and
- Of confidential advisory and deliberative communications relating to the preparation of management analysis projects conducted by the Department pursuant to State

Finance and Procurement Article, §7-103, Annotated Code of Maryland.

- Note: Privileged records may be disclosed if the information is requested by a Court of Law as defined within GP 4-301(1)

Sensitive

Sensitive is used to define information that, if divulged, could compromise or endanger the citizens or assets of the State.

If an employee is uncertain of the classification of a particular piece of information, the employee should contact their manager for clarification.

All sensitive information should be clearly identified as “Sensitive” and will be subject to the following handling guidelines.

Guidelines for Marking and Handling State-Owned Information

It is necessary to classify information so that every individual that comes in contact with it knows how to properly handle and/or protect such information. The following marking and handling requirements are applicable to public and confidential information:

Public Information:

- Marking: No marking requirements.
- Access: Unrestricted
- Distribution within Maryland state systems: No restrictions.
- Distribution outside of Maryland state systems: No restrictions.
- Storage: Standard operating procedures based on the highest security category of the information recorded on the media. (Refer to the System Security Categorization Policy in the following section).
- Disposal/Destruction: Refer to Physical Security section of this document.
- Penalty for deliberate or inadvertent disclosure: Not applicable.

Confidential Information:

- Marking: Confidential information is to be clearly identified as “Confidential”.
- Access: Only those Maryland state employees or contractors with explicit need-to-know and other individuals for whom an authorized Maryland state official has determined there is a need-to-know and an appropriate non-disclosure agreement has been obtained.
- Distribution within State of Maryland systems; Delivered direct - signature required, envelopes stamped Confidential, or an approved, electronic email or electronic file

transmission method.

- Distribution outside of State of Maryland systems: Delivered direct; signature required; approved private carriers; or approved encrypted electronic email or encrypted electronic file transmission method.
- Storage: Physically control access to system media (paper and digital) and protect confidential data using encryption technologies and/or other substantial mitigating controls (such as Data Loss Prevention, Network Security Event Monitoring, and strict database change monitoring). Storage is prohibited on portable devices and publicly accessible systems unless prior written approval from agency Secretary (or delegated authority) has been granted. Approved storage on portable devices or publicly accessible systems must be encrypted. Keep from view by unauthorized individuals; protect against viewing while in use and when unattended, store in locked desks, cabinets, or offices within a physically secured building.
- Disposal/Destruction: Dispose of paper information in specially marked disposal bins on Maryland state premises or shred; electronic storage media is sanitized or destroyed using an approved method. Refer to *Physical Security section of this document.*

Confidential information should be protected with administrative, technical, and physical safeguards designed to ensure its confidentiality and integrity and to prevent unauthorized or inappropriate access, use, or disclosure. Confidential information is prohibited on portable and non-state owned devices unless prior written approval from agency Secretary (or delegated authority) has been granted. Exceptions to this may include contracted managed (outsourced) services where security of confidential information is documented, reviewed and approved by data custodians (or delegated authority).

Approved storage on any portable device must be protected with encryption technology. When cryptography is employed within information systems, the system must perform all cryptographic operations using FIPS 140-2 validated cryptographic modules with approved modes of operation. The penalty for deliberate or inadvertent disclosure of confidential information can range from administrative actions to adverse personnel actions up to termination of employment. Deliberate, unauthorized disclosure of confidential information may result in civil and/or criminal penalties.

System Security Categorization Policy

This section defines common security category levels for information systems and provides a framework that promotes effective management and oversight of information security programs. Formulating and documenting the security level of an information system helps to determine the level of effort or controls required to protect it.

This policy applies to all information systems within the State Government. Agency officials must use the security categorizations described in FIPS Publication 199 (http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf). Additional security designators may be developed under the framework of FIPS and used at agency discretion.

The security categories are based on potential impact to an agency should certain events occur which jeopardize the information and information systems needed by that agency to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an agency.

Security Objectives

The Federal Information Security Management Act (FISMA) defines three security objectives for information and information systems:

Confidentiality

- "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542]
- A loss of *confidentiality* is the unauthorized disclosure of information.

Integrity

- "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]
- A loss of *integrity* is the unauthorized modification or destruction of information.

Availability

- "Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542]
- A loss of availability is the disruption of access to or use of information or an information system.

Potential Impact on Organizations and Individuals

FIPS Publication 199 defines three levels of potential impact (low, moderate, and high) on organizations or individuals should there be a breach of security (e.g., a loss of confidentiality, integrity, or availability). The application of these definitions must take place within the context of each organization and overall State interest.

The potential impact is LOW if—

The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

Clarification: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to agency assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

The potential impact is MODERATE if—

The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

Clarification: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the agency is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to agency assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

The potential impact is HIGH if—

The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on agency operations, organizational assets, or individuals.

Clarification: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the agency is not able to perform one or more of its primary functions; (ii) result in major damage to agency assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

The following is a checklist to help determine the categorization of an MIS. If any of the following are marked as true, the MIS should **not** be categorized as “Low” and a “Moderate” classification is likely.

Question/Criteria	Yes	No
Is there the possibility for citizens' names, addresses, age, workplace, school attended, and/or any biometric information, or any other sensitive information, to be stored or processed this system or application – ether in a structured format or in the comments field, an uploaded/attached document, or other free text?		
Could the unauthorized disclosure of any information that could possibly be stored or processed in this system or application have an adverse effect on organizational operations, organizational assets, or individuals?		
Could the unauthorized modification or destruction of any information stored or processed in this system or application could have an adverse effect on organizational operations, organizational assets, or individuals?		
Could the disruption of access to or use of information or the system or application adverse effect on organizational operations, organizational assets, or individuals?		

Security Categorization Applied to Information Systems

Determining the security category of an information system requires consideration of the sensitivity of the information resident on that system. For an information system, the potential impact values assigned to the respective security objectives (confidentiality, integrity, availability) must be considered at least 'moderate' if the information stored on them is considered 'confidential'. The generalized format for expressing the security category, SC, of an information system is: SC information system = {(confidentiality, impact), (integrity, impact), (availability, impact)}, Where the acceptable values for potential impact are LOW, MODERATE, or HIGH.

Maryland Agencies are required to maintain an inventory of security categorization designations for all information systems owned and managed by the organization.

Security Control Requirements Overview

This section defines requirements that must be met for agencies to properly protect confidential information under their administrative control. All information systems (hosted on a state network or a third-party off site premise) used for receiving, processing, storing and transmitting confidential information must be protected in accordance with these requirements. Information systems include the equipment, facilities, and people that handle or process confidential information.

This computer security framework was primarily developed using applicable guidelines specified in NIST SP 800-30, *Risk Management Guide for Information Technology Systems* and SP 800-53, *Recommended Security Controls for Federal Information Systems* and also Internal Revenue Service (IRS) Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies*. Only applicable controls designed to protect systems with a '**moderate**' category level, as defined in Federal Information Processing Standards Publication (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, are included in this policy as a baseline.

Systems with a 'high' category level should reference NIST SP 800-53 (current revision) for guidance in applying appropriate additional security controls.

This framework categorizes security controls into three types:

1. Management
2. Operational
3. Technical

Management security controls focus on managing organizational risk and information system security and devising sufficient countermeasures for mitigating risk to acceptable levels. Management security control families include risk management, security assessment and authorization, security planning, and system and services acquisition.

Operational security controls focus on mechanisms primarily implemented by people as opposed to systems. These controls are established to improve the security of a group, a specific system, or a group of systems. Operational security controls require technical or specialized expertise and often rely on management and technical controls. Operational security controls include awareness and training, configuration management, contingency planning, incident response, maintenance, media protection, physical and personnel security, and system and information integrity.

Technical security controls focus on operations executed by the computer system through mechanisms contained in the hardware, software and firmware components of the system. Technical security control families include identification and authentication, access control, audit and accountability, and system and communications protection.

Management Level Controls

Risk Management

Risk Management refers to the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. A risk management program is an essential management function and is critical for any agency to successfully implement and maintain an acceptable level of security. A risk management process must be implemented to assess the acceptable risk to agency IT systems as part of a risk-based approach used to determine adequate security for their systems. Proper risk management requires steps to be taken to reduce the risk level to an acceptable level. These steps include the initial assessment, risk mitigation and evaluation.

Risk *assessment* is the first process of risk management. Agencies must use risk assessment to determine the extent of the potential threat and the risk associated with an IT system throughout its System Development Life Cycle (SDLC). The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process. NIST SP 800-30 (R1) *Guide for Conducting Risk Assessments* provides guidance for carrying out each of the steps in the risk assessment process, such as planning, executing, communicating results, and maintaining the assessment.

Risk *mitigation*, the second process of risk management, involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process. Controls are defined as IT processes and technologies designed to close vulnerabilities, maintain continuity of operation at specified performance levels, and achieve and document compliance with policy requirements. The controls presented in this section are designed to mitigate risks and are required to comply with this policy.

The third process of risk management, *evaluation*, is ongoing and evolving. Evaluation emphasizes the good practice to develop an effective risk management program within the agency's information security program. Not only should the risk management program drive changes to existing systems, but it should also integrate into the agency's operational functions, as well as the SDLC for new systems and applications. The following table outlines the minimum DoIT security control requirements which all information systems must adhere to in order to operate in a production environment.

Security Control ID	Risk Assessment Policy and Procedures	Security Baselines		
RA-1	Maryland Agencies must develop and implement a Risk Assessment (RA) Policy/Procedure that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance as they pertain risk assessment activities within the organization. The policy/procedure must also describe how the Maryland Agency intends to implement the security requirements associated to this NIST control family. The Risk Assessment Policy/Procedure must be approved by the Maryland Agency's designated Senior Executive or Authorizing Official. The Risk Assessment Policy/Procedure must be disseminated to all state and contractor personnel with IT security responsibilities within the Maryland Agency. **The policy must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**	Low	Moderate	High
Security Categorization				
RA-2	The Maryland Agency must ensure that: a. Information and the information system are categorized in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards and guidance including FIPS 199, Standards for Security Categorization of Federal Information and Information Systems and NIST SP 800-60, (R1), Guide for Mapping Types of Information and Information Systems to Security Categories, Volumes I and II. b. Security categorization results (including supporting rationale) are documented in the system security plan for the information system. c. The security categorization decision is reviewed and approved by the AO or the AO's designated representative. d. The security categorization is subject to review and revision by the state CISO.	Low	Moderate	High

Risk Assessment				
RA-3	DoIT will ensure that: a. Assessments of the risk are conducted, including the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification, or destruction of information systems and the information they process, store, or transmit b. Risk assessment results are documented **in the Risk Assessment Report (RAR) and System Security Plan (SSP)** c. Risk assessment results are reviewed at least **annually**. d. Risk assessment results are disseminated to System Administrators, System Owners, AOs and the Chief Information Security Officer (CISO) e. The risk assessment is updated at least **annually based on one third of the security controls being assessed** or whenever there are significant changes to information systems or environments of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system. For Cloud based environments, DoIT will ensure that the following conditions are met pertaining to the Risk Assessment document: a. Awareness of where sensitive data is stored and transmitted across applications, databases, servers and network infrastructure b. Compliance with defined retention periods and end-of-life disposal requirements c. Data classification and protection from unauthorized use, access, loss, destruction, and falsification Weaknesses not readily corrected must be tracked in a system-level POA&M.	Low	Moderate	High

Vulnerability Scanning				
RA-5	The Maryland Agency must ensure that: a. Scans for vulnerabilities in information systems and hosted applications are conducted at least monthly and when recommended by the IT Security Office including when new vulnerabilities potentially affecting the system/application are identified and reported. b. Vulnerability scanning tools are employed that promote interoperability among tools and that automate parts of the vulnerability management process by using standards for: c. Ensuring platforms, software flaws, and improper configurations. d. Formatting, checklists and test procedures. e. Measuring vulnerability impact. f. Vulnerability scan reports and results from security control assessments are analyzed. g. Vulnerabilities are prioritized and remediated based on threat intelligence, compensating controls, and other factors to ensure that vulnerabilities are addressed in appropriate timeframes. h. 90 days for low systems/low risk vulnerabilities i. 60 days for moderate systems/low risk, low systems/moderate risk j. 30 days for high systems/low risk, moderate systems/moderate risk, low systems/high risk k. 15 days for high systems/moderate and high risk, moderate systems/high risk, and for all critical vulnerabilities, regardless of system classification l. This timeframe could also be modified as appropriate based on the impact level of the system, vulnerability, compensating controls and likelihood of exploits. POA&Ms must be created to track confirmed system scan vulnerabilities. For any vulnerabilities that cannot not be remediated within the applicable timeframes described above, expected remediation date and detailed remediation actions should be clearly documented in the assigned POA&M	Low	Moderate	High

	repository for tracking and managing purpose. m. Information obtained from the vulnerability scanning process and security control assessments is shared with system administrators, system owner and the CISO to help eliminate similar vulnerabilities in other information systems (e.g., systemic weaknesses or deficiencies).			
Vulnerability Scanning | Update Tool Capability				
RA-5.1	DoIT will employ vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned**.**	N/A	Moderate	High
Vulnerability Scanning| Update by Frequency/Prior to New Scan/When Identified				
RA-5.2	Update and review vulnerability definitions and signatures prior to each scan or when new vulnerabilities are identified or reported.	N/A	Moderate	High
Vulnerability Scanning| Discoverable Information				
RA-5.4	Attempts must be made to discern what information about information systems is discoverable by adversaries.	N/A	Moderate	High
Vulnerability Scanning| Privileged Access				
RA-5.5	Agencies should ensure that privileged access authorization to **servers and network devices** for more intrusive vulnerability scanning activities or scanning of sensitive system information is included to facilitate more thorough scanning.	N/A	Moderate	High

Security Assessment and Authorization

Agencies must produce an Authorization to Operate (ATO) document that verifies security controls have been adequately implemented (or plan to be implemented) to protect confidential information. The ATO constitutes the agency's acknowledgment and acceptance of risk associated with the system.

Custodians of confidential information will, via the completion of a security authorization form, verify the completeness and propriety of the security controls used to protect confidential information before initiating operations. This must be done for any infrastructure component or system associated with confidential information. This process must occur **every three (3) years** or whenever there is a **significant change** (e.g., major software upgrade, implementation of new hardware, change of hosting services, etc.) to the control structure. A senior agency official must sign and approve the security authorization.

Agencies must continuously (at least annually) monitor the security controls within their information systems to ensure that the controls are operating as intended. Agencies must authorize and document all connections from information systems to other information systems outside of the system boundary using service interface agreements and monitor/control system connections on an ongoing basis. Agencies must annually conduct a formal assessment of the security controls of information systems to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting applicable security requirements. Agencies are responsible for developing and periodically updating a Plan of Action & Milestones (POA&M) worksheet to identify any deficiencies related to the processing of confidential information and implementation of requirements. The POEM must identify planned, implemented, and evaluated remedial actions to correct deficiencies noted during annual assessments. A Corrective Action Plan (CAP) will identify activities planned or completed to correct deficiencies identified during the Security Assessment review. Both the POEM and the CAP must address implementation of security controls to reduce or eliminate known vulnerabilities in agency systems. The following table outlines the minimum DoIT security control requirements which all information systems must adhere to in order to operate in a production environment.

Security Control ID	Security Assessment and Authorization Policy and Procedures	Security Baselines		
CA-1	Maryland Agencies must develop and implement a Security Assessment and Authorization (CA) Policy/Procedure that: (a) addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance as they pertain risk assessment activities within the organization and (b) describes how the Maryland Agency intends to implement the security requirements associated with this NIST control family. The Security Assessment and Authorization Policy/Procedure must be approved by the Maryland Agency's designated Senior Executive or Authorizing Official. The Security Assessment and Authorization Policy/Procedure must be disseminated to all state and contractor personnel with IT security responsibilities within the Maryland Agency. **The policy must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**	Low	Moderate	High

Security Assessments				
CA-2	The Maryland Agency must ensure that for each information system: a. A security assessment plan is developed that describes the scope of the assessment including: ● Security controls and control enhancements under assessment ● Procedures to be used to determine security control effectiveness ● Assessment environment, assessment team, and assessment roles and responsibilities b. DoIT requires that one-third of the controls be assessed annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. A compilation of the assessments is presented to the AO as a Security Authorization Package to reauthorize the system. c. A security assessment report is produced that documents the results of the assessment d. The results of the security control assessment are provided, in writing, to the system AO or AO designated representative To satisfy the requirement, System Owners can draw from several sources, provided the sources are current and relevant to determining the security control effectiveness. These sources include but are not limited to: (i) assessments conducted as part of the information system authorization or re-authorization process; (ii) continuous monitoring activities; and (iii) testing and evaluation of information systems as part of the ongoing SDLC process.	Low	Moderate	High

Security Assessments| Independent Assessor				
CA-2.1	An independent assessor or assessment team must be employed to assess the security controls in the information system. Level/degree of assessment team independence is defined and approved by DoIT. Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of organizational information systems. Independent assessments can be obtained from elements within organizations or can be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of independence based on the security categories of information systems and/or the ultimate risk to organizational operations, organizational assets, or individuals.	N/A	Moderate	High
Security Assessments| Specialized Assessment				
CA-2.2	**Annual, announced penetration testing** must be included as a part of security control assessments. This enhancement only applies to High categorization systems. If any High systems are introduced in the future these requirements will be further defined.	N/A	N/A	High

System Interconnections				
CA-3	The Maryland Agency must ensure that all systems: a. Authorize connections from information systems to other information systems outside of their authorization boundary using Interconnection Security Agreements. b. Ensure that, for each connection, the interface characteristics, security requirements, and the nature of the information communicated are documented. ● Ensure that information system connections are monitored on an ongoing basis, verifying enforcement of security requirements. ● Ensure the connections between information systems are dedicated. ● Consider the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within the organization and external to the organization. ● Ensure an Interconnection Security Agreement (ISA) is documented and in place if one is needed. (Per current NIST SP 800-53, interconnecting systems that have the same authorizing official are not required to maintain an ISA). c. Review Interconnection Security Agreements on an **annual basis** and update as necessary.	Low	Moderate	High
System Interconnections| Restriction on External System Connections				
CA-3.5	The Maryland Agency must employ **deny-all, allow-by-exception** policy for allowing state environments and systems to connect to external information systems.	N/A	Moderate	High

Plan of Action and Milestones				
CA-5	The Maryland Agency must ensure that: a. POA&Ms are developed for information systems that document the planned remedial actions to correct weaknesses or deficiencies noted during assessments (internal and external audits or evaluations) and to reduce or eliminate known vulnerabilities in the system. b. Existing POA&Ms are updated **at least monthly** or more often based on the findings from security controls assessments, security impact analysis, and continuous monitoring activities, including POA&M remediation actions.	Low	Moderate	High
Security Authorization				
CA-6	The Maryland Agency must: a. Assign a senior-level executive or manager to the role of AO for information systems. b. Ensure the authorizing official authorizes information systems for processing before commencing operations. c. Update the security authorization **on an annual basis or upon significant change to the system that may require reauthorization.**	Low	Moderate	High

Continuous Monitoring				
CA-7	The Maryland Agency must ensure that a continuous monitoring strategy is developed and that a continuous monitoring program is implemented that includes: a. Establishment of a process that identifies information systems to be monitored and includes monitoring activities that support DoIT risk management decisions. b. Establishment of continuous monitoring and annual assessments to support such monitoring. Continuous monitoring activities should include annual reauthorization, security impact analysis, security control assessment and analysis, quarterly scans, determination of risk associated with the system vulnerabilities, remediation activities, etc. c. Ongoing security status monitoring of organization defined metrics in accordance with the continuous monitoring strategy. d. Correlation and analysis of security-related information generated by assessments and monitoring. e. Response action to address the results of the analysis of security related information. f. Reporting the security state of information systems to appropriate DoIT officials (CISO, AO) annually. A subset of security controls (1/3) is assessed **annually** during continuous monitoring and reauthorization efforts. The Agency CISO, collaborating with DoIT, establishes the selection criteria and subsequent subset for assessment.	Low	Moderate	High

Continuous Monitoring| Independent Assessment				
CA-7.1	The Maryland Agency must employ independent assessors or assessment teams to monitor the security controls in the information system on an ongoing basis. Level/degree of assessment team independence is defined and approved by the Maryland Agency. Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of organizational information systems. Independent assessments can be obtained from elements within organizations or can be contracted to public or private sector entities outside of organizations. AOs determine the required level of independence based on the security categories of information systems and/or the ultimate risk to organizational operations, organizational assets, or individuals.	N/A	Moderate	High
Penetration Testing				
CA-8	The Maryland Agency must conduct penetration testing on an annual basis on information systems containing sensitive PII.	N/A	Moderate	High
Internal System Connections				
CA-9	The Maryland Agency must ensure that: a. Information systems' internal connections are authorized. b. For each internal connection, the interface characteristics, security requirements, and the nature of the information communicated are documented.	Low	Moderate	High

Planning

Agency security planning controls include system security plans and system security plan (SSP) updates. Agencies must develop, document, and establish a system security plan by describing the implementation needed to meet security requirements, current controls and planned controls for protecting agency information systems and confidential information. The system security plan must be updated on a regular basis to account for significant changes in the security requirements, current controls and planned controls for protecting agency information systems and confidential information. IT security planning is an important quality control tool that helps improve the protection level of IT assets. All state systems have some level of sensitivity and require protection as part of good management practices. The IT security planning process encompasses the following components:

- Documentation of security and privacy controls in an SSP
- System Authorization
- Security training, awareness, and education

When an AO authorizes system operation, they are accepting the associated risk of information loss, system misuse, unauthorized system access or modification, system unavailability, and undetected system activities. Good security planning, therefore, serves an important risk management function by providing the necessary information to determine the type and level of risks, and to base decisions on risk acceptance or mitigation. Managers must also be assured that all personnel accessing the system, from those performing system management functions to general users, have received security training at levels commensurate with the duties they perform. The following table outlines the minimum DoIT security control requirements which all information systems must adhere to in order to operate in a production environment.

Security Control ID	Security Planning Policy and Procedures	Security Baselines		
PL-1	Maryland Agencies must develop and implement a Security Planning (PL) Policy/Procedure that: (a) addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance as they pertain to risk assessment activities within the organization and (b) describes how the Maryland Agency intends to implement the security requirements associated with this NIST control family. The Security Planning Policy/Procedure must be approved by the Maryland Agency's designated Senior Executive or Authorizing Official. The Security Planning Policy/Procedure must be disseminated to all state and contractor personnel with IT security responsibilities within the Maryland Agency. **The policy must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**	Low	Moderate	High

System Security Plan				
PL-2	The Maryland Agency must ensure that: a. A security plan is developed for the information system that: 1. Is consistent with the organization's enterprise architecture 2. Explicitly defines the authorization boundary for the system 3. Describes the operational context of the information system in terms of missions and business processes 4. Provides the security categorization of the information system including supporting rationale 5. Describes the operational environment for the information system and relationship with or connections to the other information systems 6. Provides an overview of the security requirements for the system 7. Identifies any relevant overlays, if applicable 8. Describes the security controls in place or planned for meeting those requirements (including a rationale for tailoring and supplementation decisions) 9. Is reviewed and approved by the SO, CISO, CTO and AO, **prior to plan implementation** b. Copies of the security plan are distributed and any subsequent changes to the plan are communicated to the designated Maryland officials such are SO, CISO, CTO and AO. c. Security plans for information systems are reviewed **at least annually**. d. The plan is updated to address changes to information systems/environments of operation or problems identified during plan implementation or security control assessments. a. The security plan is protected from unauthorized disclosure and modification.	Low	Moderate	High

System Security Plan| Plan/Coordinate with Other Organizational Entities				
PL-2.3	The Maryland Agency must ensure that security related activities (security assessments, audits, hardware and software maintenance, contingency planning, vulnerability and compliance scanning, etc.) affecting the information system are planned and coordinated with the Cybersecurity personnel, system owners, technical leads/system administrators, etc.before conducting such activities in order to reduce the impact on other organizational entities.	N/A	Moderate	High
Rules of Behavior				
PL-4	The Maryland Agency must ensure that: a. All personnel read the Acceptable Use Policy which outlines expected behavior and responsibilities about information and information systems usage. The Acceptable Use Policy is readily available to all Maryland employees and individuals requiring access to the information system including personnel with administrative privileges to ensure they handle the elevated privileges properly. b. Signed acknowledgements are received from users indicating that they have read, understand, and agree to abide by the Acceptable Use Policy before authorizing access to information and information system. c. The Acceptable Use Policy is reviewed and updated on an annual basis. d. Individuals who have signed a previous version of the Acceptable Use Policy are required to read and resign when the rules are revised and updated.	Low	Moderate	High
Rules of Behavior| Social Media and Networking Restrictions				
PL-4.1	The Maryland Agency must include in the Acceptable Use Policy, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.	N/A	Moderate	High

Information Security Architecture				
PL-8	The Maryland Agency must ensure that system owners: a. Develop an information security architecture for the information system that: 1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of system information. 2. Describes how the information security architecture is integrated into and supports the enterprise architecture. 3. Describes any information security assumptions about, and dependencies on, external services. b. Review and update the information security architecture **at least annually** to reflect updates in the enterprise architecture. c. Ensure that planned information security architecture changes are reflected in the security plan, the security Concept of Operations, and organizational procurements/acquisitions.	Low	Moderate	High

Service Interface Agreements

External network connections may be permitted only after all approvals are obtained consistent with this policy and must be managed in accordance with a Service Interface Agreement (SIA) that is agreed to by the state agency and the untrusted entity. Specific criteria should be included in an SIA regarding the system IT Security. An SIA must include, at a minimum:

- Purpose and duration of the connection as stated in the agreement, lease, or contract;
- Points-of-contact and cognizant officials for both the State and untrusted entities;
- Roles and responsibilities of points-of-contact and cognizant officials for both the State and untrusted entities;
- Security measures to be implemented by the untrusted organization to protect the State's IT assets against unauthorized use or exploitation of the external network connection; and
- Requirements for notifying a specified state official within a specified period (4 hours recommended) of a security incident on the network.

Operational Level Controls

Awareness and Training

Agencies must ensure all information system users and managers are knowledgeable of security awareness material before authorizing access to systems. Agencies must identify personnel with information system security roles and responsibilities, document those roles and responsibilities, and provide sufficient security training before authorizing access to information systems or confidential information. Agencies must document and monitor individual information system security training activities including basic security awareness training and specific information system security training. The following table outlines the minimum DoIT security control requirements which all information systems must adhere to in order to operate in a production environment.

Security Control ID	Security Awareness and Training Policy and Procedures	Security Baselines		
AT-1	Maryland Agencies must implement a Security Awareness and Training (AT) Policy/Procedure that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance as they pertain to risk assessment activities within the organization. The policy/procedure must also describe how the Maryland Agency intends to implement the security requirements associated to this NIST control family. The Security Awareness and Training Policy/Procedure must be approved by the Maryland Agency's designated Senior Executive or Authorizing Official. The Security Awareness and Training Policy/Procedure must be disseminated to all state and contractor personnel with IT security responsibilities within the Maryland Agency. **The policy must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**	Low	Moderate	High

Security Awareness Training				
AT-2	All Maryland Agency information system users (including but not limited to managers, senior executive staff and contractors) must complete basic information system security awareness training/materials as part of initial training for new users **within 30 days of appointment** and **before authorizing access to the system**. In addition, security awareness training is required to be performed due to significant information system changes. Basic security awareness training must be provided and completed **annually** thereafter.	Low	Moderate	High
Security Awareness| Insider Threat				
AT-2.2	The Maryland Agency must include security awareness training upon recognizing and reporting potential indicators of insider threat. Potential indicators and possible precursors of insider threat can include behaviors such as inordinate, long-term job dissatisfaction, attempts to gain access to information not required for job performance, unexplained access to financial resources, bullying or sexual harassment of fellow employees, workplace violence, and other serious violations of organizational policies, procedures, directives, rules, or practices, etc.	N/A	Moderate	High

Role-Based Security Training				
AT-3	The Maryland Agency must require that all personnel with assigned security roles and responsibilities are provided role-based security- related training: a. **Before authorizing access** to any information system b. **Before performing assigned duties** that may require access to FTI c. **When required by system changes** d. **At least annually** thereafter. Content of security training must be based on assigned roles and responsibilities and the specific requirements of the Maryland Agency and the information systems to which personnel have authorized access.	Low	Moderate	High
Security Training Records				
AT-4	The Maryland Agency must ensure that: a. Individual information systems security training activities, including basic security awareness training and specific information systems security training are documented and monitored. b. Individual training records are retained for **5 years (current year, plus 4 past years)**. c. Contractors are included in the agency's security training process, especially those who have access to FTI.	Low	Moderate	High

Configuration Management

System hardening procedures must be created and maintained to ensure up-to-date security best practices are deployed at all levels of the IT systems (operating systems, applications, databases and network devices). All default system administrator passwords must be changed. Agencies must implement an appropriate change management process to ensure changes to the systems are controlled by:

- Developing, documenting, and maintaining current secured baseline configurations.
- Network devices should be patched and updated for all security related updates/patches using automated tools when possible.
- Develop, document, and maintain a current inventory of the components of information systems and relevant ownership information.
- Configuring information systems to provide only essential capabilities.
- Configuring the security settings of information technology products to the most restrictive mode consistent with operational requirements.
- Analyzing potential security impacts of changes prior to implementation.
- Authorizing, documenting, and controlling system level changes.
- Restricting access to system configuration settings and provide the least functionality necessary.
- Prohibiting the use of functions, ports, protocols, and services not required to perform essential capabilities for receiving, processing, storing, or transmitting confidential information.
- Maintaining backup copies of hardened system configurations.

Configuration management describes the processes through which baseline configurations are developed and maintained for information systems and their constituent components. System configurations must be compliant with DoIT security requirements, and all changes to system configurations must be controlled and approved. The process of configuration management provides for a controlled environment in which changes to software and hardware are properly authorized, tested, and approved before implementation. The following table outlines the minimum DoIT security control requirements which all Maryland information systems must adhere to in order to operate in a production environment.

Security Control ID	Configuration Management Policy and Procedures	Security Baselines		
CM-1	Maryland Agencies must develop and implement a Configuration Management (CM) Policy/Procedure that: (a) addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance as they pertain to risk assessment activities within the organization and (b) describes how the Maryland Agency intends to implement the security requirements associated with this NIST control family. The Configuration Management Policy/Procedure must be approved by the Maryland Agency's designated Senior Executive or Authorizing Official. The Configuration Management Policy/Procedure must be disseminated to all state and contractor personnel with IT security responsibilities within the Maryland Agency. **The policy must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**	Low	Moderate	High

Baseline Configuration				
CM-2	Baseline documentation must exist for all systems within scope. The Maryland Agency must ensure that current baseline configurations of information system components are developed, documented, and maintained under configuration control. **NOTE:** For The Maryland Agency applications, the configuration guides or equivalent documentation should document the following; ● Versions of Compilers used ● Build options when creating application/components ● Versions of COTS Software Used as part of the application ● For web applications, which browsers and what versions are supported ● All Known security assumptions, implications, system level protections, best practices, and required permissions ● Deployment configuration settings ○ Encryption settings (data in transit) ○ PKI Certificate Configuration Settings ○ Password Settings	Low	Moderate	High
Baseline Configuration| Reviews and Updates				
CM-2.1	Baseline configuration documentation must be reviewed and updated: a. **At least annually.** b. When required due to **system upgrades, patches, or other significant system change.** c. As an integral part of information system component installations and upgrades.	N/A	Moderate	High

Baseline Configuration| Automation Support for Accuracy/Currency				
CM-2.2	Automated mechanisms must be employed for network devices, critical systems and other information system components to maintain up- to-date, complete, accurate, and readily available baseline configurations. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Baseline Configuration| Retention of Previous Configurations				
CM-2.3	At a **minimum, a single iteration** of the previous baseline configuration baseline configurations must be retained as deemed necessary to support rollback. Retaining previous versions of baseline configurations to support rollback may include, for example, hardware, software, firmware, configuration files, and configuration records. Versions of host/instances are maintained through AWS versioning. Tape is used to store all data for baseline configuration.	N/A	N/A	High

Baseline Configuration| Configure Systems, Components, or Devices for High Risk Areas				
CM-2.7	Access to the Maryland Agency network resources and systems from foreign countries is currently prohibited. No information systems or system components may be used during foreign travel to perform government related work. a. Where an exception to this policy is needed, then approval must be obtained from Agency Senior management through a request submitted well in advance. Reference the DoIT IT Security Guidelines for International Travel for more information on international travel requirements. b. The Maryland Agency must ensure the following if approval is to be provided: c. No personally owned mobile devices will be used on foreign travel to perform government related work. d. Only DoIT approved and furnished mobile devices are allowed. e. Approved foreign travel devices including any removable media must be configured to encrypt stored data using FIPS 140-2 validated encryption. f. Device must provide protection against malware. g. Travelers must ensure physical security of the device while in transit and while on foreign travel or foreign duty. h. Loss, theft or compromise of assigned mobile devices while on travel should be immediately reported to the Maryland Agency's Incident Response Team (IRT).	Low	Moderate	High

Configuration Change Control				
CM-3	The Maryland Agency must ensure that: a. The types of changes to information systems that are configuration controlled are determined. b. Configuration-controlled changes to information systems are reviewed and approved or disapproved with explicit consideration for security impact analyses. c. Configuration- change decisions associated with the information system are documented. d. Approved configuration-controlled changes to the information system are implemented. e. Records of configuration control changes to the information system are retained for the life of the system. f. Activities associated with configuration-controlled changes to the information systems are audited and reviewed **at least quarterly.** g. Oversight for configuration change control activities is coordinated and provided through the Agency Configuration Control Board that **convenes weekly to review upcoming configuration changes.**	N/A	Moderate	High

Configuration Change Control| Automated Document/Notification/Prohibition of Changes				
CM-3.1	Automated mechanisms must be employed to: a. Document proposed changes to information systems. b. Notify and request approval from designated approval authorities. c. Highlight approvals that have not been received **in the time period specified in the Configuration Control Board process document.** d. Prohibit change until necessary approvals are received. e. Document completed changes to information systems. f. Notify organization designated individuals when approved changes to the information system are completed. This enhancement only applies to High categorization systems. If any High systems are introduced this requirement will be further defined.	N/A	N/A	High
Configuration Change Control| Test/Validate/Document Changes				
CM-3.2	Changes to information systems must be tested, validated, and documented before being implemented on the operational system.	N/A	Moderate	High
Security Impact Analysis				
CM-4	It is required that any changes to information systems must be analyzed to determine the potential security impacts prior to implementing the change.	Low	Moderate	High
Security Impact Analysis| Separate Test Environment				
CM-4.1	Changes to critical information systems providing essential services to Agencies and constituents, must be analyzed in a separate test environment before installation in an operational environment. This analysis must look for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.	Low	Moderate	High

Access Restrictions for Change				
CM-5	Physical and logical access restrictions associated with changes to information systems must be defined, documented, approved, and enforced. The Maryland Agency must ensure a formal approval process is in place for granting individuals the authority to perform system changes.	N/A	Moderate	High
Access Restrictions for Change| Automated Access Enforcement/Auditing				
CM-5.1	The Maryland Agency information systems must enforce access restrictions and support auditing of the enforcement actions. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Access Restrictions for Change| Review System Changes				
CM-5.2	Information system changes must be reviewed monthly and when significant changes to the system occur to determine if unauthorized changes have occurred. Access rights to the configuration management repository must be periodically reviewed, at **least semi-annually**. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Access Restrictions for Change| Signed Components				
CM-5.3	Information systems must prevent the installation of patches, service packs, and device drivers that are not signed with a certificate that is recognized and approved by DoIT. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High

Configuration Settings				
CM-6	The Maryland Agency must ensure that: a. Mandatory configuration settings for the information technology products employed within information systems are established and documented using checklists that reflect the most restrictive mode consistent with operational requirements (CIS benchmarks, IRS SCSEMs, etc.) b. Configuration settings are implemented. c. Deviations from the established configuration settings for individual components within information systems including servers, workstations, network components, databases, etc. are identified, documented, and approved based on explicit operational requirements which are documented in the information system SSP and/or Secure Configuration Baseline. d. Changes to configuration settings are monitored and controlled.	Low	Moderate	High
Configuration Settings| Automated Central Management/Application/Verification				
CM-6.1	The Maryland Agency must employ automated mechanisms to centrally manage, apply, and verify the configuration settings for servers and network devices. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Configuration Settings| Respond to Unauthorized Change				
CM-6.2	The Maryland Agency must ensure that organization defined safeguards are employed to respond to unauthorized changes to required established information system configuration settings. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High

Least Functionality				
CM-7	The Maryland Agency must ensure that information systems are configured to provide only essential capabilities and specifically prohibit or restrict settings that are deemed unnecessary or non-secure functions, ports, protocols, and/or services which do not align with CIS Benchmarks.	Low	Moderate	High
Least Functionality| Periodic Review				
CM-7.1	Information systems must be reviewed **at least monthly**, to identify and disable unnecessary or non-secure functions, ports, protocols, and/or services such as FTP, Peer to Peer networking, Bluetooth, etc.	N/A	Moderate	High
Least Functionality| Prevent Program Execution				
CM-7.2	The Maryland Agency must ensure that the information systems prohibit unauthorized or unapproved software from executing on information system components according to approved software list and Change Advisory Board (CAB) approval.	N/A	Moderate	High

Least Functionality| Unauthorized Software/Blacklisting				
CM-7.4	The Maryland Agency must ensure that: a) Software programs that are not authorized to execute on the information system are identified and documented. DoIT employs white list that identifies all software authorized to execute on the information system. All software not listed on the whitelist is deemed as prohibited (performed through Trend Micro) i. The use of software and associated documentation is tracked and protected in accordance with contract agreements and copyright laws. b) **deny-all, allow-by-exception policy** is employed to prohibit the execution of unauthorized software programs on the information system i. The use of peer-to-peer file sharing technology must be controlled and documented to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. c) The list of unauthorized software programs is reviewed and updated on an **at least an annual basis**. The agency also establishes restrictions on the use of open source software. Open source software must: a) Be legally licensed b) Approved by the agency's IT department c) Adhere to a secure configuration baseline checklist from the US Government or industry.	N/A	Moderate	High

Least Functionality| Authorized Software/Whitelisting				
CM-7.5	The Maryland Agency must ensure that: a. The list of software programs authorized to execute on the information system is identified. b. Deny-all, permit-by-exception policy is employed to allow the execution of authorized software programs on the information system. c. The list of authorized software programs is reviewed and updated on an annual basis. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High

Information System Component Inventory				
CM-8	Inventory of information system components must be: a. developed, documented, and maintained and must: 1. Accurately reflect the current information system. 2. Include all components within the authorization boundary of the information system that store, process or transmit FTI, PII, PHI, or other sensitive information. 3. Be at the level of granularity deemed necessary for tracking and reporting. b. Include the following information: 1. Inventory requirements for system hardware: 2. Point of Contact or Owner 3. Instance tag or Serial Number 4. Operating System (OS) Vendor Name 5. Operating System (OS) Version Number 6. Operating System (OS) Patch Level 7. Fully Qualified Domain Name (FQDN) 8. IP Address/Hostname 9. Make and Model when applicable 10. Physical Location c. Inventory requirements for system software for servers, workstations, and laptops of various kinds and uses in production and pre-production environments: 1. Point of Contact 2. Software Vendor Name 3. Software Version Number Reviews and updates of the information system component inventory should be done **at least annually or when information system changes occur.**	Low	Moderate	High

Information System Component Inventory| Updates During Installations/Removals				
CM-8.1	Inventories of information systems components must be updated as an integral part of component installations, removals, and information system updates.	N/A	Moderate	High
Information System Component Inventory| Automated Maintenance				
CM-8.2	Automated mechanisms must be employed to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Information System Component Inventory| Automated Unauthorized Component Detection				
CM-8.3	The Maryland Agency must ensure that: a. Automated mechanisms are employed **quarterly** to detect the addition of unauthorized hardware, software and firmware components with the information system. b. Network access by such components/devices is disabled and designated Maryland Agency officials (System Owners, CISO, etc.) are notified when deviations or unauthorized software is discovered.	N/A	Moderate	High
Information System Component Inventory| Accountability Information				
CM-8.4	Means for identifying by name individuals responsible for administering information system components should be included in property accountability information for those components. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High

Information System Component Inventory| No Duplicate Accounting of Components				
CM-8.5	The Maryland Agency must ensure that all components within the authorization boundary of each information system are either inventoried as a part of the system and should not duplicate in other information system inventory or are recognized by another system as a component within that system.	N/A	Moderate	High
Configuration Management Plan				
CM-9	The Maryland Agency must ensure that a configuration management plan for information systems is developed, documented, and implemented that: a. Addresses roles, responsibilities, and configuration management processes and procedures, b. Establishes process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items. c. Defines the configuration items for the information system and places the configuration items under configuration management. d. Protects the configuration management plan from unauthorized disclosure and modification.	N/A	Moderate	High

Software Usage Restrictions				
CM-10	The Maryland Agency must ensure that: a. Software and associated documentation is used in accordance with contract agreements and copyright laws, b. The use of software and associated documentation protected by quantity licenses is tracked to control copying and distribution. c. The use of peer-to-peer software and file sharing services is controlled and documented to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. d. The use of open source software is controlled and documented to address the software is legally licensed, approved by the agency IT department and adheres to secure configuration baseline checklist(s) provided by the US Government.	Low	Moderate	High
User Installed Software				
CM-11	The Maryland Agency must ensure that: a. Policies documenting permitted and prohibited actions regarding software installation and procedural enforcement methods governing the installation of software by users are established. b. Software installation policies are enforced through automated methods, implementation of least privilege and periodic review of user accounts. Only authorized users are given necessary privileges to install software. c. Policy compliance is monitored on a semi-annual basis, or as significant changes occur.	Low	Moderate	High

Contingency Planning

State agencies must have a plan in place to minimize the risk of disruption to services due to system unavailability. Contingency planning details the necessary procedures required to protect the continuing performance of business functions and services, including IT services, during an outage to successfully restore and operate systems and business functions during significant disruption. Creation, maintenance, and annual testing of a plan will minimize the impact of recovery and loss of information assets caused by events ranging from a single disruption of business to a disaster. Planning and testing provides a foundation for a systematic and orderly resumption of all computing services within an agency when disaster strikes.

Primary Components of an IT Contingency Plan are:

- Identification of a disaster/contingency team;
- Definitions of recovery team member responsibilities;
- Documentation of each critical system including;
    - Purpose
    - Hardware
    - Operating System
    - Application(s)
    - Data
    - Supporting network infrastructure and communications
    - Identity of person responsible for system restoration
- System restoration priority list;
- Description of current system back-up procedures;
- Description of back-up storage location;
- Description of back-up testing procedures (including frequency);
- Identification of disaster recovery site including contact information;
- System Recovery Time Objective (RTO);
- System Recovery Point Objective (RPO) (how current should the data be?); and
- Procedures for system restoration at backup and original agency site.

The following table outlines the minimum DoIT security control requirements which all Maryland information systems must adhere to in order to operate in a production environment.

Security Control ID	Contingency Planning Policy and Procedures	Security Baselines		
CP-1	Maryland Agencies must: (a) develop and implement a Contingency Planning (CP) Policy/Procedure that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance as they pertain risk assessment activities within the organization and (b) describe how the Maryland Agency intends to implement the security requirements associated to this NIST control family. The Contingency Planning Policy/Procedure must be approved by the Maryland Agency's designated Senior Executive or Authorizing Official. The Contingency Planning Policy/Procedure must be disseminated to all state and contractor personnel with IT security responsibilities within the Maryland Agency. **The policy must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**	Low	Moderate	High

Contingency Plan				
CP-2	The Maryland Agency must ensure that: a. Contingency plans are developed for information systems that: 1. Identify essential missions and business functions and associated contingency requirements. 2. Provide recovery objectives, restoration priorities, and metrics. 3. Address contingency roles, responsibilities, and assigned individuals with contact information. 4. Address maintaining essential missions and business functions despite an information system disruption, compromise, or failure. 5. Address eventual, full information system restoration without deterioration of the security measures originally planned and implemented. 6. Are reviewed and approved by designated Maryland Agency officials such a Senior Executive or Authorizing Official. b. Copies of contingency plans are distributed to **personnel identified in the system contingency plans**. c. Contingency plan activities are coordinated with incident handling activities. d. Contingency plans are reviewed and approved **at least annually.** e. Contingency plans are updated to address changes to the Agency, information systems, or environment of operation and problems encountered during contingency plan implementation, execution, or testing. f. Contingency plan changes are communicated to **personnel identified in the system contingency plans.** g. The contingency plan is protected from unauthorized disclosure and modification.	Low	Moderate	High

Contingency Plan| Coordinate with Related Plans				
CP-2.1	The Maryland Agency must ensure that contingency plan development is coordinated with organizations responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, and Incident Response Plan, Emergency Action Plan).	N/A	Moderate	High
Contingency Plan| Capacity Planning				
CP-2.2	The Maryland Agency must ensure that capacity planning is conducted so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Contingency Plan| Resume Essential Business/Mission Function				
CP-2.3	Plans must exist for the resumption of essential missions and business functions within the time frame specified in the system **contingency plan** after activation of the contingency plan.	N/A	Moderate	High
Contingency Plan| Resume All Missions/ Business Functions				
CP-2.4	The Maryland Agency must ensure that the resumption of all missions and business functions within the time frame specified in the system contingency plan of contingency plan activation is adequately planned. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High

Contingency Plan| Continue Essential Missions/Business Functions				
CP-2.5	The Maryland Agency must plan for the continuance of essential missions and business functions with little or no loss of operational continuity until full information system restoration at primary processing and/or storage sites. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Contingency Plan| Identify Critical Assets				
CP-2.8	The Maryland Agency must identify all critical information system assets supporting essential missions and business functions.	N/A	Moderate	High
Contingency Training				
CP-3	Contingency training documentation must identify roles and responsibilities of organizational personnel when assuming a contingency role and responsibility. Training must be provided to information system users consistent with assigned roles and responsibilities **no later than ninety (90) days** of assuming a contingency role or responsibility; when required by information system changes; and at **least annually thereafter**. Training content must include: a. Information regarding when and where to report for duty during contingency operations and if normal duties are affected. b. Role based training for system administrators who may require additional training on how to set up information systems at alternate processing and storage sites. c. Role based training for managers/senior leaders who may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activity.	Low	Moderate	High

Contingency Training| Simulated Events				
CP-3.1	Contingency training must incorporate simulated events to facilitate effective responses by personnel in crisis situations. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Contingency Plan Testing				
CP-4	The Maryland Agency must ensure that: a. Contingency plans for the information system are tested and/or exercised **at least annually** using **DoIT defined tests, or exercises** to determine the plan's effectiveness and the Maryland Agency's readiness to execute the plans. b. Contingency plan test/exercise are documented, and the results are reviewed. c. Corrective actions are initiated as needed.	Low	Moderate	High
Contingency Plan Testing| Coordinate with Related Plans				
CP-4.1	Contingency plan testing and/or exercises must be coordinated with DoIT organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, and Incident Response Plan, Emergency Action Plan).	N/A	Moderate	High
Contingency Plan Testing| Alternate Processing Site				
CP-4.2	Contingency plans must be tested at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High

Alternate Storage Site				
CP-6	The Maryland Agency must: a. Establish an alternate storage site, including necessary agreements to permit storage of information systems backup information. b. Alternate storage sites should provide information security safeguards equivalent to that of the primary site.	N/A	Moderate	High
Alternate Storage Site| Separation From Primary Site				
CP-6.1	Alternate storage sites must be separated from the primary storage site in order to reduce susceptibility to the same threats including natural disasters, structural failures, hostile cyber-attacks etc. Agencies should determine what is considered a sufficient degree of separation between primary and alternate storage sites based on the types of threats that are of concern and business continuity requirements.	N/A	Moderate	High
Alternate Storage Site| Recovery Time/Point Objectives				
CP-6.2	Alternate storage sites must be configured to facilitate recovery operations in accordance with recovery time and recovery point objectives. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Alternate Storage Site| Accessibility				
CP-6.3	Potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster must be identified and explicit mitigation actions must be outlined.	N/A	Moderate	High

Alternate Processing Site				
CP-7	The Maryland Agency must ensure that: a. An alternate processing site is established, including necessary agreements to permit the transfer and resumption of all critical information system operations for essential missions and business functions **within the time frame identified by each Agency, based on their business continuity requirements (to be captured in a Business Impact Analysis (BIA))**, when primary processing capabilities are unavailable. b. Equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site in time to support system transfer/resumption within the defined time period. c. The alternate processing site provides information security safeguards equivalent to that of the primary site.	N/A	Moderate	High
Alternate Processing Site| Separation From Primary Site				
CP-7.1	Alternate processing sites must be separated from the primary processing site in order to reduce susceptibility to the same threats including for example natural disasters, structural failures, hostile cyber-attacks, etc. Agencies should determine what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats that are of concern.	N/A	Moderate	High
Alternate Processing Site| Accessibility				
CP-7.2	Potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster must be identified and explicit mitigation actions must be outlined. **NOTE:** Potential accessibility problems to the alternate processing site and mitigation procedures can be documented in either the System Security Plan, contingency plan, or other relevant Agency Alternate Processing Site documentation.	N/A	Moderate	High

Alternate Processing Site| Priority of Service				
CP-7.3	The Maryland Agency must ensure that alternate processing site agreements that contain priority of service provisions in accordance with the DoIT 's availability requirements including recovery time objectives are developed.	N/A	Moderate	High
Alternate Processing Site| Preparation for Use				
CP-7.4	The Maryland Agency should ensure that the alternate processing site is prepared and ready to be used as the operational site supporting essential missions and business functions. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Telecommunication Services				
CP-8	The Maryland Agency must ensure that alternate telecommunications services are established, including necessary agreements to permit resumption of all critical information systems operations for essential missions and business functions within **twenty-four (24)** hours when primary telecommunication capabilities are unavailable at either the primary or alternate processing or storage sites. The resumption of information system operations for critical mission/business functions must be continued throughout or resumed rapidly after a disruption of normal activities.	N/A	Moderate	High

Telecommunications Services| Priority of Service Provision				
CP-8.1	The Maryland Agency must ensure that: a. Primary and alternate telecommunication service agreements are developed that contain priority-of- service provisions in accordance with the DoIT 's availability requirements including recovery time objective. b. Telecommunications Service Priority is requested for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.	N/A	Moderate	High
Telecommunications Services| Single Points of Failure				
CP-8.2	Alternate telecommunications services need to be obtained in order to reduce the likelihood of sharing a single point of failure with primary telecommunications services.	N/A	Moderate	High
Telecommunications Services| Separation of Primary/Alternate Providers				
CP-8.3	The Maryland Agency must ensure that alternate telecommunications services are obtained from providers that are separated from primary service providers in order to reduce susceptibility to the same threats. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Telecommunications Services| Provider Contingency Plan				
CP-8.4	The Maryland Agency must ensure that: a) Primary and alternate telecommunications service providers have adequate contingency plans. b) Such contingency plans are reviewed to ensure that the plans meet DoIT contingency requirements. c) Evidence of contingency testing/training by providers is obtained **annually**. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High

Information System Backup				
CP-9	The Maryland Agency must ensure that: a. Backups of user-level information, system-level information (including system state information), and information system documentation including security-related documentation contained in the information system are conducted **at least weekly.** b. The confidentiality, integrity and availability of backup information is protected using encryption, access controls, etc. when at the storage location. When backup information is in transit, the use of cryptographic mechanisms with a key **no less than 128 bits in length, or FIPS 140-2 compliant**, whichever is stronger, is required.	Low	Moderate	High
Information System Backup| Testing for Reliability/Integrity				
CP-9.1	Back-up information must be tested **at least annually** to verify media reliability and information integrity.	N/A	Moderate	High
Information System Backup| Test Restoration Using Sampling				
CP-9.2	A sample of backup information must be used in the restoration of selected information system functions as part of contingency plan testing. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined	N/A	N/A	High
Information System Backup| Separate Storage for Critical Information				
CP-9.3	Back-up copies of the operating system and other critical information system software, as well as copies of the information system inventory (including hardware, software, and firmware components), must be stored in a separate facility or in a fire-rated container that is not collocated with the operational system. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High

Information System Backup| Transfer to Alternate Storage Site				
CP-9.5	The Maryland Agency must ensure that on premise information system backup information is transferred to an alternate storage site **on a monthly basis** at a transfer rate consistent with the recovery point objectives. For cloud based platforms, this control is not applicable. Alternate storage sites in the clouds do not exist, as the management of backups is configured and maintained via automated processes. In the cloud, backups are dispersed throughout the organization defined geographical regions. Full backups in the cloud must occur **on a daily basis** at a transfer rate consistent with the recovery point objectives.	Low	Moderate	High
Information System Recovery and Reconstitution				
CP-10	The Maryland Agency must provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. For Agency applications, testing should occur at **least annually**, and results recorded to verify security remains in place when an application failure occurs.	Low	Moderate	High
Information System Recovery and Reconstitution| Transaction Recovery				
CP-10.2	All Maryland Agency transaction-based information systems must implement transaction recovery.	N/A	Moderate	High
Information System Recovery and Reconstitution| Restore Within Time Period				
CP-10.4	The Maryland Agency must ensure the capability to restore information system components within the time frame defined in the system contingency plans from configuration-controlled and integrity-protected information representing a known, operational state for the components is provided. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High

Incident Response

Information Technology Incident Management refers to the processes and procedures agencies implement for identifying, responding to, and managing information security incidents. A computer incident within Maryland state government is defined as a violation of computer security policies, acceptable use policies, or standard computer security practices. Refer to NIST SP 800-61 Revision 2 *Computer Security Incident Handling Guide* for guidance in creating an incident management policy and developing plans and procedures to support it.

To clearly communicate incidents and events (any observable occurrence in a network or system), it is necessary for the agency incident response teams to adopt a common set of terms and relationships between those terms. All elements of state government should use a common taxonomy, per the definitions of terms, roles, and procedures contained in this document. System owners and the Maryland state CISO are kept informed of system vulnerability advisories from the US Computer Emergency Readiness Team (US-CERT), from software vendors, and other sources and should communicate this information to relevant individuals and Agencies. The process also must ensure tracking and implementation of corrective actions (e.g., developing filter rules and patching) and coordinates with responsible incident response capabilities regarding the handling and reporting of incidents involving systems under the program area's responsibility.

Agencies must report IT incidents to DoIT and the Maryland state CISO by completing an IT Incident Report (Appendix A) and provide as much information about the incident as possible including: the incident category, how the incident was discovered, affected IP addresses, port numbers, information about the affected agency system, impact to the agency, and the final resolution. The following table outlines the minimum DoIT security control requirements which all Maryland information systems must adhere to in order to operate in a production environment.

Security Control ID	Incident Response Policy and Procedures	Security Baselines		
IR-1	Maryland Agencies must develop and implement an Incident Response (IR) Policy/Procedure that: (a) addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance as they pertain risk assessment activities within the organization and (b) describes how the Maryland Agency intends to implement the security requirements associated with this NIST control family. The Incident Response Policy/Procedure must be approved by the Maryland Agency's designated Senior Executive and Authorizing Official. The Incident Response Policy/Procedure must be disseminated to all state and contractor personnel with IT security responsibilities within the Maryland Agency. **The policy must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**	Low	Moderate	High
Incident Response Training				
IR-2	Incident response training must be provided to information system users consistent with assigned roles and responsibilities within: a. **30 Days** of assuming an incident response role or responsibility b. When required **by information system changes** c. **At least annually** thereafter	Low	Moderate	High
Incident Response Training| Simulated Events				
IR-2.1	Simulated events should be incorporated into incident response training to facilitate effective personnel response in crisis situations. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High

Incident Response Training| Automated Training Environments				
IR-2.2	Automated mechanisms should be employed to provide a more thorough and realistic training environment. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Incident Response Testing				
IR-3	The Maryland Agency must ensure the incident response capability for the information systems is tested and/or exercised **at least annually** using tests and/or exercises defined by CISO or outlined in the test plan and test results are documented. DoIT has defined two types of tests: ● **Tabletop Exercises** – Tabletop exercises are facilitated, discussion-based exercises where personnel meet to discuss roles, responsibilities, coordination, and decision-making of a given scenario. ● **Functional Exercises** – Functional exercises allow personnel to validate their readiness for emergencies by performing their duties in a simulated environment. NIST SP 800-61 revision 2 provides sample scenarios for incident response teams to use for tabletop testing exercises. The type of scenario tested must be different than the previous tested scenario (e.g., year one performs Tabletop exercise, year two perform Functional exercise). The test must be conducted in as close to an operational environment as possible; if feasible, an actual virtual test of the components or systems used to conduct daily operations for the organization should be used. The scope of testing can range from individual system components or systems to comprehensive tests of all information systems and components that support an IT plan.	Low	Moderate	High

Incident Response Testing| Coordination with Related Plans				
IR-3.2	The Maryland Agency must coordinate incident response testing with organizational elements responsible for related plans (Contingency Plans, Business Continuity Plans, etc.).	N/A	Moderate	High
Incident Handling				
IR-4	The Maryland Agency must ensure that: a. An incident handling capability for security incidents is implemented that includes preparation, detection and analysis, containment, eradication, and recovery. b. Incident handling activities are coordinated with contingency planning activities. c. Lessons learned from ongoing incident handling, activities are incorporated into incident response procedures, training, and testing/exercising, and that the resulting changes are implemented accordingly.	Low	Moderate	High
Incident Handling| Automated Incident Handling Process				
IR-4.1	The Maryland Agency must employ automated mechanisms to support the incident handling process.	N/A	Moderate	High
Incident Handling| Information Correlation				
IR-4.4	The Maryland Agency must correlate incident information and individual incident responses to achieve an organization- wide perspective on incident awareness and response. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Incident Monitoring				
IR-5	The Maryland Agency must ensure information system security incidents are tracked and documented on an ongoing basis.	Low	Moderate	High

Incident Monitoring| Automated Tracking/Data Collection/Analysis				
IR-5.1	Automated mechanisms must be employed to assist in tracking security incidents and in the collection and analysis of incident information.	Low	Moderate	High
Incident Reporting				
IR-6	The Maryland Agency must: a. Require personnel to report a suspected or verified security incident to the DoIT incident response team (DoIT IRT) immediately upon discovery. b. Ensure that security incident information is reported to the DoIT IRT as applicable. The Agency Incident Response Team performs an initial investigation and determines whether the event should be considered a security incident. If the event is not a computer security or privacy incident, DoIT will manage the event according to its internal procedures. c. Confirmed computer security incidents and suspected or confirmed privacy incidents will be reported within established timelines to the US-CERT. In addition to reporting requirements within the State of Maryland, incidents involving PII or FTI may be required to be reported to the following federal agencies, based on the type of data involved and the associated reporting requirements: ● US Department of Health and Human Services ● Administration for Children and Families ● Office of Child Support Enforcement Security ● The Social Security Administration (SSA) ● Appropriate special agent-in-charge at the Treasury Inspector General for Tax Administration (TIGTA) ● IRS Office of Safeguards	Low	Moderate	High

Incident Reporting| Automated Reporting				
IR-6.1	The Maryland Agency must employ automated mechanisms to assist in reporting security incidents.	N/A	Moderate	High
Incident Response Assistance				
IR-7	The Maryland Agency must provide an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.	Low	Moderate	High
Incident Response Assistance| Automation Support For Availability of Information/Support				
IR-7.1	The Maryland Agency must employ automated mechanisms to increase the availability of incident response-related information and support.	N/A	Moderate	High

Incident Response Plan				
IR-8	The Maryland Agency must ensure that: a. An incident response plan is developed that: 1. Provides the Agency with a roadmap for implementing its incident response capability. 2. Describes the structure and organization of the incident response capability. 3. Provides a high-level approach for how the incident response capability fits into the overall DoIT. 4. Meets the unique Agency requirements due to factors such as mission, size, structure, and functions. 5. Defines reportable incidents. 6. Provides metrics for measuring the incident response capability within the Agency. 7. Defines the resources and management support necessary to effectively maintain and mature an incident response capability. 8. Is reviewed and approved by designated DoIT officials. b. Copies of the incident response plan are distributed to System Owners, Managers, CISO, CTO, and other key personnel as deemed necessary. c. The incident response plan is reviewed **annually**. d. The incident response plan is updated to address changes to information systems or problems encountered during plan implementation, execution, or testing. e. Incident response plan changes are communicated to System Owners, Managers, CISO, CTO, etc. f. Incident response plan is protected from unauthorized disclosure and modification.	Low	Moderate	High

Information Spillage Response				
IR-9	Agencies, with oversight from DoIT, should examine the information spillage procedures and determine if the procedures detail the agency approach toward managing spillage if a specific information system is contaminated. These procedures must address the following; a. Identifying the specific information involved in the information system contamination. b. Alerting agency officials of the information spill. c. Isolating the contaminated information system or system component. d. Following proper sanitization procedures to remove the information from the contaminated information system or component. e. Identifying other information systems or system components that may have been subsequently contaminated.	Low	Moderate	High

Maintenance

Maintenance controls are used to monitor software installation and updates to ensure that systems function as expected, and that a historical record of changes is maintained. Maintenance controls are also used to limit the type of software installed on systems to prevent the installation and use of unauthorized software on IT systems. Agencies must identify, approve, control, and routinely monitor the use of information system maintenance tools and remotely executed maintenance and diagnostic activities on a regular basis. Agencies must ensure that system maintenance is scheduled, performed, and documented in accordance with manufacturer or vendor specifications and/or organizational requirements. Only authorized personnel are to perform maintenance on information systems. The following table outlines the minimum DoIT security control requirements which all Maryland information systems must adhere to in order to operate in a production environment.

Security Control ID	Maintenance Policy and Procedures	Security Baselines		
MA-1	Maryland Agencies must develop and implement a Maintenance (MA) Policy/Procedure that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance as they pertain risk assessment activities within the organization. The policy/procedure must also describe how the Maryland Agency intends to implement the security requirements associated to this NIST control family. The Maintenance Policy/Procedure must be approved by the Maryland Agency's designated Senior Executive or Authorizing Official. The Maintenance Policy/Procedure must be disseminated to all state and contractor personnel with IT security responsibilities within the Maryland Agency. **The policy must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**	Low	Moderate	High

Controlled Maintenance				
MA-2	The Maryland Agency must ensure that: a. Scheduling, performance, documentation, and review of records of maintenance and repairs on information system components is conducted in accordance with manufacturer or vendor specifications and/or DoIT requirements. b. All maintenance activities are approved and monitored, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location. c. The system owner explicitly approves the removal of information systems or information system components from DoIT facilities for off-site maintenance or repairs as applicable, excluding Hard Disk Drives (HDD) of any kind. DoIT does not allow the HDD to be removed from the DoIT Facility for any reason. d. Functioning equipment is sanitized to remove all information from associated media prior to removal from DoIT facilities for off-site maintenance or repairs; Hard disk drives (HDD) are excluded and not permitted to be sent off site. e. All potentially impacted security controls are checked to verify that the controls are still functioning properly following maintenance or repair actions. f. Date and time of maintenance, name of individual or group performing maintenance, description of maintenance performed, information system components removed or replaced during the maintenance, and name of escort if necessary should be included in the maintenance record.	Low	Moderate	High

Controlled Maintenance| Automated Maintenance Activities				
MA-2.2	Automated mechanisms must be employed to schedule, conduct, and document maintenance and repairs required, producing up-to-date, accurate and complete records of all maintenance and repair actions requested, scheduled, in process and completed. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Maintenance Tools				
MA-3	The Maryland Agency approves, controls and monitors information system maintenance tools.	N/A	Moderate	High
Maintenance Tools| Inspect Tools				
MA-3.1	All maintenance tools (e.g., diagnostic and test equipment) carried into Maryland Agency facilities by maintenance personnel must be inspected for improper and unauthorized modifications.	N/A	Moderate	High
Maintenance Tools| Inspect Media				
MA-3.2	All media containing diagnostic and test programs (e.g., software or firmware used for system maintenance or diagnostics) must be checked for malicious code before the media is used in the information systems.	N/A	Moderate	High
Maintenance Tools| Prevent Unauthorized Removal				
MA-3.3	The Maryland Agency must prevent the unauthorized removal of maintenance equipment containing organizational information by: a. Verifying that there is no Maryland information contained on the equipment. b. Sanitizing or destroying the equipment. c. Retaining the equipment within the facility. d. Obtaining an exemption from designated personnel explicitly authorizing removal of the equipment from the facility. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High

Non-Local Maintenance				
MA-4	The Maryland Agency must ensure that: a. Third Parties and unvetted personnel complete approved non-local maintenance and diagnostics activities through chaperoned access, using an approved screen sharing tool from a station dedicated to providing this access. b. The use of non-local maintenance and diagnostic tools is allowed only if consistent with DoIT policy and as documented in information system security plans and have been approved as a part of an authority to operate (ATO). c. Strong authenticators are employed in the establishment of non-local maintenance and diagnostic sessions. d. Records are maintained for non-local maintenance and diagnostic activities through the ITSM and recorded when possible using screen recording software. e. All sessions and network connections are terminated when non-local maintenance is completed.	Low	Moderate	High
Non-Local Maintenance| Document Nonlocal Maintenance				
MA-4.2	The policies and procedures for the establishment and use of non-local maintenance and diagnostic connections should be documented in information system security plan.	N/A	Moderate	High

Non-Local Maintenance| Comparable Security/Sanitization				
MA-4.3	The Maryland Agency must ensure that either: a. Non-local maintenance and diagnostic services are performed from an information system that implements a level of security at least as high as that implemented on the system being serviced; or b. The component to be serviced are removed from the information system and sanitized (with regard to DoIT information) prior to non-local maintenance or diagnostic services and before removal from DoIT facilities, and inspected and sanitized (with regard to potentially malicious software and surreptitious implants) after the service is performed and before reconnecting the component to the information system. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Maintenance Personnel				
MA-5	The Maryland Agency must ensure that: a. A process for authorizing maintenance personnel on-site is established and a list of personnel authorized to perform maintenance on information systems is adequately maintained. Only authorized personnel must perform maintenance on information systems. b. Non-escorted personnel performing maintenance on information systems have required access authorizations. c. Organization designates personnel with required access authorization and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorization.	Low	Moderate	High

Maintenance Personnel| Individuals Without Appropriate Access				
MA-5.1	The Maryland Agency must: a. Implement procedures for the use of maintenance personnel that lack appropriate security clearances or are not US citizens, that include the following requirements: 1. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified. 2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured. b. Develop and implement alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High

Timely Maintenance				
MA-6	System Owners must ensure that maintenance support and/or spare parts for information system components are obtained within **48 hours or less of failure** or as otherwise defined in maintenance agreements and the system contingency plan or operational support plan. Security-critical components may include, for example, firewalls, guards, gateways, intrusion detection systems, audit repositories, authentication servers, and intrusion prevention systems.	N/A	Moderate	High

Media Protection

The purpose of this section is to ensure proper precautions are in place to protect confidential information stored on media.

All media that contains confidential information including removable media (CDs, magnetic tapes, external hard drives, flash/thumb drives, DVDs, copier hard disk drives, and information system input and output (reports, documents, data files, back-up tapes) must be clearly labeled “Confidential”. Agencies must restrict access to system media containing confidential information to authorized individuals.

Media labeled “Confidential” must be physically controlled and securely stored.

Agencies must protect and control “Confidential” system media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

Agencies must deploy a tracking method to ensure “Confidential” system media reaches its intended destination.

When no longer required for mission or project completion, media to be used by another person within the agency must be overwritten (clear or purge) with software and protected consistent with the classification of the data. Specific procedures must be documented in the applicable agency IT System Security Plan.

Throughout the lifecycle of IT equipment, there are times when an agency will be required to relinquish custody of the asset. The transfer of custody may be temporary, such as when the equipment is serviced or loaned, or the transfer may be permanent; examples being a donation, trade-in, lease termination or disposal through GovDeals.com. Any transfer of custody of equipment poses a significant risk that confidential information, licensed software or intellectual property stored on that equipment may also be transferred.

To eliminate the possibility of inadvertently releasing residual representation of state data, state agencies must either destroy the electronic storage media (provide evidence of destruction documentation) or ensure that the electronic storage media has been sanitized in accordance with NIST SP800-88 (R1), *Guidelines for Media Sanitization*.

Note: Disposal of electronic storage media should be in compliance with the agency’s document retention policy and litigation hold procedures.

Several factors should be considered along with the security categorization of the

system when making sanitization decisions. Disposal decisions should be made based upon the classification of the data, level of risk, and cost to the agency. The following table outlines the minimum DoIT security control requirements which all Maryland information systems must adhere to in order to operate in a production environment.

Security Control ID	Media Protection Policy and Procedures	Security Baselines		
MP-1	Maryland Agencies must develop and implement a Media Protection (MP) Policy/Procedure that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance as they pertain risk assessment activities within the organization. The policy/procedure must also describe how the Maryland Agency intends to implement the security requirements associated to this NIST control family. The Media Protection Policy/Procedure must be approved by the Maryland Agency's designated Senior Executive or Authorizing Official. The Media Protection Policy/Procedure must be disseminated to all state and contractor personnel with IT security responsibilities within the Maryland Agency. **The policy must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**	Low	Moderate	High
Media Access				
MP-2	The Maryland Agency must ensure that access to digital and non-digital media is restricted to authorized users through an approved access control list. Digital media may include, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm.	Low	Moderate	High

Media Marking				
MP-3	The Maryland Agency must ensure that removable information system media and information system output are marked indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information. This excludes any media or output that is considered non-sensitive.	N/A	Moderate	High
Media Storage				
MP-4	The Maryland Agency must ensure that: a. All digital and non-digital information system media are physically controlled and securely stored within DoIT controlled areas using approved access control lists. b. Information system media is protected until the media are destroyed or sanitized using approved equipment, techniques, and procedures. Digital media may include, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes for example, handwritten notes, paper files, still photographs, and other types of printed media.	N/A	Moderate	High

Media Transport				
MP-5	The Maryland Agency must ensure that: a. Both digital and nondigital media are protected and controlled during transport outside of controlled area using DoIT defined security safeguards. b. Accountability for information system media is maintained during transport outside of controlled areas. c. Activities associated with the transport of information system media is documented. d. Activities associated with transport of such media are restricted to authorized personnel. Sensitive information in hardcopy or removable media must not be removed from DoIT premises without prior authorization. Digital media may include, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes for example, handwritten notes, paper files, still photographs, and other types of printed media.	Low	Moderate	High
Media Transport| Cryptographic Protection				
MP-5.4	The Maryland Agency must require cryptographic mechanisms that are FIPS 140-2 compliant and consistent with FIPS Publication 140-2 Annex A in order to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	N/A	Moderate	High

Media Sanitization				
MP-6	The Maryland Agency must: a. Sanitize information system media, both digital and non-digital, prior to disposal, release from DoIT control, or release for reuse using defined sanitization techniques consistent with NIST SP 800-88 (R1). b. Employ sanitization mechanisms with strength and integrity commensurate based on the security categorization and classification of the system information. For cloud services, the Maryland Agency must ensure that the cloud provider uses acceptable physical destruction methods to include, for example; a. Disintegration b. Incineration c. Pulverizing d. Shredding e. Melting f. Wiping This applies to all information system media, both digital and nondigital, subject to disposal or reuse, whether or not the media is considered removable. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices.	Low	Moderate	High
Media Sanitization| Review/Approve/Track/Document/Verify				
MP-6.1	Media sanitization and disposal actions must be approved, tracked, documented, and verified.	Low	Moderate	High
Media Sanitization| Equipment Testing				
MP-6.2	Media sanitization equipment and procedures must be tested **at least annually** to verify that the intended sanitization is being achieved.	Low	Moderate	High

Media Sanitization| Nondestructive Techniques				
MP-6.3	Portable, removable storage devices must be sanitized upon issuance and reissuance prior to connecting such devices to information systems.	Low	Moderate	High
Media Use				
MP-7	The Maryland Agency must restrict the use of flash drives or external hard drives on all workstations and mobile devices using technical and/or non-technical safeguards. Only DoIT approved portable storage devices that are FIPS 140-2 certified should be used.	Low	Moderate	High
Media Use| Prohibit Use Without Owner				
MP-7.1	The Maryland Agency must prohibit the use of portable storage devices in organizational information systems when such devices have no identifiable owner.	N/A	Moderate	High

Physical and Personnel Security

Physical security refers to the provisions of a safe and secure environment for information processing activities. Physical access to information technology processing equipment, media storage areas, and media storage devices and supporting infrastructure (communications, power, and environmental) must be controlled to prevent, detect, and minimize the effects of unauthorized or unintended access to these areas.

Physical access controls must be in place for the following:

- Data Centers;
- Areas containing servers and associated media;
- Networking cabinets and wiring closets;
- Power and emergency backup equipment; and
- Operations and control areas.

Each agency is responsible for:

- Ensuring proper employee/contractor identification processes are in place;
- Conducting background investigations during the hiring process
- Ensuring proper environmental and physical controls are established to prevent accidental or unintentional loss of information residing on IT systems; and
- Ensuring that any physical access controls are auditable.
- Ensuring that employees/contractors receive annual training in regards to physical security best practices.

The following table outlines the minimum DoIT security control requirements which all Maryland information systems must adhere to in order to operate in a production environment.

Security Control ID	Physical and Environmental Protection Policy and Procedures	Security Baselines		
PE-1	Maryland Agencies must develop and implement a Physical and Environmental Protection (PE) Policy/Procedure that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance as they pertain risk assessment activities within the organization. The policy/procedure must also describe how the Maryland Agency intends to implement the security requirements associated to this NIST control family. The Physical and Environmental Protection Policy/Procedure must be approved by the Maryland Agency's designated Senior Executive or Authorizing Official. The Physical and Environmental Protection Policy/Procedure must be disseminated to all state and contractor personnel with IT security responsibilities within the Maryland Agency. **The policy must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**	Low	Moderate	High

Physical Access Authorizations				
PE-2	The Maryland Agency must ensure that: A. A current list of personnel with authorized access to the facility where the information system resides is developed, approved and maintained. B. Appropriate authorization credentials (e.g., badges, identification cards, smart cards) are issued for facility access. C. The access list detailing authorized facility access by individuals is reviewed **at least annually**. D. When access is no longer required individuals are removed from the facility access list. E. Agencies enforce physical access authorizations to the information system in addition to the physical access controls where FTI is received, processed, stored, or transmitted.	Low	Moderate	High

Physical Access Control				
PE-3	The Maryland Agency must ensure that: A. For environments containing systems categorized as Low and above: ○ Physical access authorizations are enforced for all physical access points including designated entry/exit facility access points and interior access points to the information system and components by: ○ Verifying individual access authorization before granting access to the facility. B. For environments containing systems categorized as Medium and above: ○ Physical access audit logs for all physical access points including designated entry and exit facility points and interior access points where the information system resides are maintained. ○ Access to areas officially designated as publicly accessible is controlled as appropriate (in accordance with the conducted risk assessment) using organization defined safeguards (security cameras) ○ Visitors are escorted, and visitor activities are monitored when maintenance is performed on DoIT devices by outside vendors that do not have DoIT required access authorization. ○ Keys and other physical access devices are secured. ○ Controlling ingress/egress to the facility using methods including automated turnstiles, electronically locking doors, security cameras and/or guard stations. ○ Physical access devices including keys, locks, card readers etc. are inventoried at least annually. ○ Keys are changed when keys are lost, combinations are compromised, or individuals are transferred or terminated.	Low	Moderate	High

Physical Access Control| Information System Access				
PE-3.1	Physical access authorizations to information systems must be enforced independent of the physical access controls for facilities. An additional layer of physical access security must be provided for areas that are more vulnerable due to a concentration of information system components such as server rooms and communication centers (this does not apply to workstations or peripheral devices dispersed throughout the facility). This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Access Control for Transmission Medium				
PE-4	The Maryland Agency must ensure that access to all information system distribution and transmission lines within facilities hosting Maryland information systems is controlled to prevent accidental damage, disruption, and physical tampering. Physical access should be controlled by employing following safeguards: locked wiring closets, protection of cabling by conduit or cabling trays etc. Protections are implemented to prevent eavesdropping or in transit modification of unencrypted transmissions.	N/A	Moderate	High
Access Control for Output Devices				
PE-5	The Maryland Agency must ensure that physical access to information systems is controlled to prevent unauthorized individuals from obtaining information system outputs. Monitors, printers, and audio devices are examples of information system output devices.	N/A	Moderate	High

Monitoring Physical Access				
PE-6	The Maryland Agency must ensure that: a. Physical access to the facility where the information systems reside is monitored to detect and respond to physical security incidents. b. Physical access logs are reviewed **monthly** and any time physical security incidents occur (suspicious physical activities such as excessive access outside of normal work hours, repeated access to areas not normally accessed, out of sequence access, etc.) c. Results of reviews and investigations are coordinated with the DoIT 's incident response capability.	Low	Moderate	High
Monitoring Physical Access| Intrusion Alarms/Surveillance Equipment				
PE-6.1	The Maryland Agency must monitor physical intrusion alarms and surveillance equipment.	N/A	Moderate	High
Monitoring Physical Access| Monitoring Physical Access to Information Systems				
PE-6.4	The Maryland Agency must monitor physical access to the information system in addition to the physical access monitoring of the facility organization-defined physical spaces containing one or more components of the high-risk information system.	N/A	Moderate	High

Visitor Access Records				
PE-8	The Maryland Agency must ensure, for facilities that are protected by the State of Maryland, that: a. Visitor access records to the facility where the information system resides are maintained for 3 years. Visitor access logs should include the following information: 1. Name and organization of person visiting 2. Signature of the visitor and Form of identification 3. Date of access 4. Time of entry 5. Time of departure (only applicable to areas designated to process Title 26 data) 6. Purpose of visit 7. Name and organization of person visited b. Visitor access records are reviewed at least monthly.	Low	Moderate	High
Visitor Access Records| Automated Records Maintenance/Review				
PE-8.1	The Maryland Agency must employ automated mechanisms to facilitate the maintenance and review of visitor access records. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Power Equipment and Cabling				
PE-9	The Maryland Agency must ensure power equipment and power cabling for information systems are protected from damage and destruction.	N/A	Moderate	High

Emergency Shutoff				
PE-10	The Maryland Agency must ensure that within facilities containing information system resources (e.g., data center, server rooms, mainframe rooms): a. The capability of shutting off power to information systems or individual system components in emergency situations is provided. b. Emergency shutoff switches or devices in facilities containing information system resources are placed in designated locations to facilitate safe and easy access for personnel. c. Emergency power shutoff capability is protected from unauthorized activation.	N/A	Moderate	High
Emergency Power				
PE-11	The Maryland Agency must ensure provision of a short-term uninterruptible power supply to facilitate an orderly shutdown of information systems in the event of a primary power source loss.	N/A	Moderate	High
Emergency Power| Long-Term Alternate Power Supply – Minimal Operational Capability				
PE-11.1	The Maryland Agency must ensure provision of a long-term alternate power supply for information systems that can maintain minimally required operational capability in the event of an extended loss of the primary power source.	N/A	Moderate	High
Emergency Lighting				
PE-12	The Maryland Agency must ensure that automatic emergency lighting systems that activate in the event of a power outage or disruption, and cover emergency exits and evacuation routes within facility are employed and maintained.	Low	Moderate	High

Fire Protection				
PE-13	The Maryland Agency must employ and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source.	Low	Moderate	High
Fire Protection| Detection Devices/Systems				
PE-13.1	The Maryland Agency must ensure that fire detection devices/systems activate **automatically** and notify designated officials and emergency responders in the event of a fire. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Fire Protection| Suppression Devices/Systems				
PE-13.2	Fire suppression devices/systems should provide **automatic notification** of any activation to designated Maryland Agency officials and emergency responders. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Fire Protection| Automatic Fire Suppression				
PE-13.3	An **automatic** fire suppression capability must be employed for information systems when facilities are not staffed on a continuous basis.	N/A	Moderate	High

Temperature and Humidity Controls				
PE-14	The Maryland Agency must ensure that: a. Temperature and humidity levels within facilities containing information systems are maintained between **72- and 80-degrees** Fahrenheit and humidity levels maintained between **5% to 45% year-round**. b. Temperature and humidity controls are monitored regularly.	Low	Moderate	High
Water Damage Protection				
PE-15	The Maryland Agency must ensure protection of information systems from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.	Low	Moderate	High
Water Damage Protection| Automation Support				
PE-15.1	Automatic mechanisms should be employed to detect the presence of water in the vicinity of the information system and to alert designated Maryland Agency personnel. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Delivery and Removal				
PE-16	The Maryland Agency must ensure that information system hardware that is considered accountable property entering and exiting the facility is authorized, monitored, and controlled. Appropriate records of those items must be maintained.	Low	Moderate	High

Alternate Work Site				
PE-17	The Maryland Agency must ensure: a. Employment of security controls at alternate work sites. b. Assessment, as feasible, of the effectiveness of security controls at alternate work sites. c. Provision of means for employees to communicate with information security personnel in case of security incidents or problems.	N/A	Moderate	High
Location of Information System Components				
PE-18	The Maryland Agency must ensure that all information system components are positioned within facilities to minimize the potential damage from physical and environmental hazards (fire, earthquakes, flooding, electrical interference, etc.) and to minimize the opportunity for unauthorized access.	N/A	N/A	High

System and Information Integrity

Agencies must implement system and information integrity security controls including flaw remediation, information system monitoring, information input restrictions (such as validating input in all Web applications), and information output handling and retention. Integrity controls protect data from accidental or malicious alteration or destruction and ensure users that the quality and reliability of the information meets expectations.

It is expected that agencies protect against malicious code (e. g. viruses, worms, Trojan horses, etc.) by implementing (anti-virus, anti-malware) solutions that, to the extent possible, includes a capability for automatic updates. Intrusion detection/prevention tools, techniques and additional security protection mechanisms should be in place to be in compliance with DoIT requirements. The following table outlines the minimum DoIT security control requirements which all Maryland information systems must adhere to in order to operate in a production environment.

Security Control ID	System and Information Integrity Policy and Procedures	Security Baselines		
SI-1	Maryland Agencies must develop and implement a System and Information Integrity (SI) Policy/Procedure that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance as they pertain risk assessment activities within the organization. The policy/procedure must also describe how the Maryland Agency intends to implement the security requirements associated to this NIST control family. The System and Information Integrity Policy/Procedure must be approved by the Maryland Agency's designated Senior Executive or Authorizing Official. The System and Information Integrity Policy/Procedure must be disseminated to all state and contractor personnel with IT security responsibilities within the Maryland Agency. **The policy must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**	Low	Moderate	High

Flaw Remediation				
SI-2	The Maryland Agency must ensure that: a. Information system flaws are identified, reported, and corrected. b. Software and firmware updates related to flaw remediation are tested for effectiveness and potential side effects on Maryland information systems before installation. c. Security relevant software and firmware updates should be installed within 15/30/60/90 days based on severity and associated risk to the confidentiality of sensitive data and FTI. NOTE: Schedules for the installation of security relevant software and firmware updates may vary based on specific operational requirements as defined in platform-specific patching schedules; additionally, some critical patches and updates may be installed more expeditiously at the discretion of the organization. d. Flaw remediation is incorporated into the configuration management processes. The details of these requirements, specific configuration settings, and manual checks can be found on the Office of Safeguards website. For additional information regarding this control, refer to the DoIT Patch Management Policy.	Low	Moderate	High
Flaw Remediation| Central Management				
SI-2.1	The flaw remediation process must be centrally managed. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw remediation security controls. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High

Flaw Remediation| Automated Flaw Remediation Status				
SI-2.2	Automated mechanisms must be employed to determine the state of information system components with regard to flaw remediation **upon demand and no less than quarterly**.	N/A	Moderate	High
Malicious Code Protection				
SI-3	The Maryland Agency must ensure that information systems: a. Employ malicious code protection mechanisms at information system entry and exit points (firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices) to detect and eradicate malicious code transported by email, email attachments, and web accesses. b. Update malicious code protection mechanism whenever new releases are available in accordance with DoIT configuration management policy and procedures. c. Configure malicious code protection mechanisms to; 1. Perform periodic **weekly scans** of the information system and **real-time scans** of files from external sources at endpoints and network entry/exit points as the files are downloaded, opened, or executed in accordance with DoIT security policy 2. Block malicious code, quarantine malicious code, and send an alert to a system administrator in response to malicious code detection d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.	Low	Moderate	High

Malicious Code Protection| Central Management				
SI-3.1	The Maryland Agency must ensure malicious code protection mechanisms are centrally managed.	N/A	Moderate	High
Malicious Code Protection| Automatic Updates				
SI-3.2	Information systems should automatically update malicious code protection mechanisms (including signature definitions) or administrators manually push updates to all machines on a **daily basis**. After applying an update, each system must verify that it has received its signature update.	N/A	Moderate	High

Information System Monitoring				
SI-4	The Maryland Agency must: a. Monitor all information systems quarterly to detect: 1. Attacks and indicators of potential attacks in accordance with System and Information Integrity procedures requirements. 2. Unauthorized local, network, and remote connection. 3. Installations of unauthorized software. 4. Rogue hosts on the environment. 5. Unauthorized use of IT systems on workstations and servers b. Identify unauthorized use of information system through intrusion detection/prevention (IDS/IPS) systems, malicious code protection software, scanning tools, audit records monitoring, etc. c. Deploy monitoring devices: (i) strategically within the information system to collect DoIT determined essential information; and (ii) at ad hoc locations within the system to track specific types of transaction of interest to DoIT. d. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion. e. Heighten the level of information system monitoring activity whenever there is an indication of increased risk to DoIT operations and assets, individuals, other organizations, or the nation based on law enforcement information, intelligence information, or other credible sources of information. f. Obtain legal opinion with regards to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations. g. Provide monitoring information output, including records of possible attack indicators, possible unauthorized use and connections to the CISO and DoIT Cybersecurity Division as needed. h. Notify Administrators by real-time alerts or e-mail notices when potentially malicious traffic is identified.	Low	Moderate	High

Information System Monitoring| Automated Tools for Real-time Analysis				
SI-4.2	Automated tools must be employed to support near real-time analysis of events.	N/A	Moderate	High
Information System Monitoring| Inbound and Outbound Communications Traffic				
SI-4.4	Inbound and outbound communications traffic must be monitored in near real time for unusual or unauthorized activities or conditions at the external boundary of the network and at the Demilitarized Zone (DMZ) to discover anomalies such as large file transfers, long-time persistent connections, unusual or not explicitly allowed protocols and ports, and attempted communications with suspected malicious external IP addresses.	N/A	Moderate	High
Information System Monitoring| System-Generated Alerts				
SI-4.5	Information systems must alert system administrators in real-time or by an email notification when the following indications of compromise or potential compromise occur: ● Failed login attempts (>3 attempts or with account lockout) ● Security Policy Changes ● Account Changes ● Audit Logs Cleared ● Unauthorized packets based on suspected attack ● Attempt to bypass system security mechanisms ● Access to selected privileged files and applications ● Any other activities inconsistent with typical pattern of use Alerts must be written to local and remote consoles, and the administrator must acknowledge the alert. The alert and acknowledgement should be logged.	N/A	Moderate	High

Security Alerts, Advisories, and Directives				
SI-5	The Maryland Agency must ensure: a. Information system security alerts, advisories, and directives are received from designated external organizations such as US-Cert and vendor specific alerts on an ongoing basis. b. Internal security alerts, advisories, and directives are generated, analyzed and documented with the appropriate action to take as deemed necessary. c. Security alerts, advisories, and directives are disseminated to the CISO, CTO, security administrators, systems administrators, external service providers and mission/business partners. d. Security directives are implemented in accordance with established time frames or notification is sent to the issuing organization of the degree of noncompliance.	Low	Moderate	High
Security Alerts, Advisories, and Directives| Automated Alerts and Advisories				
SI-5.1	Automated mechanisms must be employed to make security alert and advisory information available throughout DoIT as needed. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Security Function Verification				
SI-6	The Maryland Agency information systems should verify the correct operation of organization defined security functions; perform verification of system startup, restart, shutdown, upon command with appropriate privileges. When anomalies are discovered, either the system administrator must be notified, or the system must shut down or restart.	Low	Moderate	High

Software, Firmware, and Information Integrity				
SI-7	The Maryland Agency must employ integrity verification tools to detect unauthorized changes to Unix and Windows servers including: a. Windows log transfer configuration or UNIX Syslog parameters b. NTP values c. SNMP values d. Local Admin accounts/User groups e. Continuous monitoring client parameters f. Information tampering g. Errors h. Omissions during system startup	N/A	Moderate	High
Software, Firmware, and Information Integrity| Integrity Checks				
SI-7.1	The Maryland Agency must ensure that information systems perform an integrity check of any anomalies, Windows log transfer configuration or Unix syslog parameters, NTP and SNMP values, local admin accounts/user groups and continuous monitoring client parameters **at least semi-annually.**	N/A	Moderate	High
Software, Firmware, and Information Integrity| Automated Notification of Integrity Violations				
SI-7.2	Automated tools should be employed to provide notification to designated individuals upon discovering discrepancies during integrity verification. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Software, Firmware, and Information Integrity| Automated Response to Integrity Violations				
SI-7.5	The Maryland Agency must ensure that information systems automatically either shut the information system down; or trigger audit alerts when integrity violations are discovered. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High

Software, Firmware, and Information Integrity| Integration of Detection and Responses				
SI-7.7	The Maryland Agency must ensure that information systems incorporate the detection of unauthorized changes to established configuration settings and unauthorized elevation of information system privileges into the organizational incident response capability.	N/A	Moderate	High
Software, Firmware, and Information Integrity| Binary or Machine Executable Code				
SI-7.14	The Maryland Agency must: a. Prohibit the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code. b. Provide exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Spam Protection				
SI-8	The Maryland Agency must ensure that: a. Spam protection mechanisms are employed at information system entry and exit points (examples include, but not limited to firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, mobile devices, and notebook/laptop computers) to detect and act on unsolicited messages. b. Spam protections are updated **when new releases are available** in accordance with DoIT configuration management policy and procedures.	N/A	Moderate	High
Spam Protection| Central Management				
SI-8.1	Spam protection mechanisms should be centrally managed.	N/A	Moderate	High

Spam Protection| Automatic Updates				
SI-8.2	The Maryland Agency information systems should automatically update spam protection mechanisms.	N/A	Moderate	High
Information Input Validation				
SI-10	The Maryland Agency information systems must check information inputs for accuracy, completeness, and validity. This is applicable to both user and automated input. Data that does not match the required format and content are rejected.	N/A	Moderate	High
Error Handling				
SI-11	The Maryland Agency information systems must: a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries. b. Reveal error messages only to authorized personnel such as system administrators. Detailed error outputs, and error outputs that include sensitive information, must be adequately protected. For applications, DoIT should also ensure applications are secure during startup and shutdown, as well as conduct fuzz testing prior to application releases.	N/A	Moderate	High
Information Handling and Retention				
SI-12	The Maryland Agency must handle and retain information within the information system and information output from the system based on business need and limited to authorized users. Data is to be stored for only the amount of time required by applicable state and federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. The handling of information by individuals is to align with the principle of least privilege, where users only have the access required to perform the minimum set of actions, based on business requirements and processes.	Low	Moderate	High

Memory Protection				
SI-16	All Maryland Agency information systems must implement memory protection on system components through the use of either hardware or software based data execution prevention and address space layout randomization to protect its memory from unauthorized code execution.	N/A	Moderate	High

Technical Level Controls

Access Control Requirements

Logical access controls are the system-based mechanisms used to designate whom or what is to have access to a specific system resource and the type of transactions and functions that are permitted. They include controls that:

- Manage user accounts, including activation, deactivation, changes and audits.
- Restrict users to authorized transactions and functions
- Limit network access and public access to the system
- Enforce assigned authorizations that control system access and the flow of information within the system and between interconnected systems.
- Identify, document and approve specific user actions that can be performed without identification or authentication
- Enforce separation of duties.
- Enforce technical limitations which can prevent unauthorized access to system resources, etc.

The following table outlines the minimum DoIT security control requirements which all Maryland information systems must adhere to in order to operate in a production environment.

Security Control ID	Access Control Policy and Procedures	Security Baselines		
AC-1	Maryland Agencies must develop and implement an Access Control (AC) Policy/Procedure that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance as they pertain risk assessment activities within the organization. The policy/procedure must also describe how the Maryland Agency intends to implement the security requirements associated to this NIST control family. The Access Control Policy/Procedure must be approved by the Maryland Agency's designated Senior Executive or Authorizing Official. The Access Control Policy/Procedure must be disseminated to all state and contractor personnel with IT security responsibilities within the Maryland Agency. **The policy must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**	Low	Moderate	High

Account Management				
AC-2	All Maryland information systems must manage information system accounts by: 1. Identifying account types (e.g., individual, group, system, application, and temporary); **NOTE**: Guest/Anonymous accounts are not permitted. Access is limited to individuals with a valid business purpose. 2. Assigning account managers for information system accounts; 3. Establishing conditions for group membership. 4. Identifying authorized users of the information system and specifying access privileges/authorizations and other attributes for each account. 5. Ensuring an approval process is in place which requires appropriate approvals from system administrators for requests to establish accounts. 6. Creating, enabling, modifying, disabling, terminating and removing information system accounts in accordance with this policy and any associated DoIT account management procedures. 7. Monitoring the use of information system accounts. 8. Monitoring and maintaining the use of service accounts. 9. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need to-know/need-to-share changes. 10. Authorizing access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions. 11. Reviewing accounts for compliance with account management requirements at least annually; Privileged accounts are reviewed at least semi-annually.	Low	Moderate	High

Account Management| Automated System Account Management				
AC-2.1	Automated mechanisms should be employed to support the management of information system accounts.	N/A	Moderate	High
Account Management| Removal of Temporary/Emergency Accounts				
AC-2.2	Temporary access to all Maryland systems will be automatically **disabled within 24 hours**, excluding weekends and federal holidays, of the end of the designated temporary access period. The designated temporary access period should not exceed **30** days.	N/A	Moderate	High
Account Management| Disable Inactive Accounts				
AC-2.3	Information systems must automatically disable inactive accounts after **60 days of inactivity**. DoIT allows for a manual process to compensate for the automated functionality. New accounts that are not used within the first **30 days** will be disabled.	N/A	Moderate	High
Account Management| Automated Audit Actions				
AC-2.4	Automated mechanisms should be employed to ensure that account creation, modification, disabling, permission changes, and termination actions are audited. Also, as required, appropriate individuals must be notified (system administrators and managers). These audit records should be reviewed on a routine basis, **at least quarterly**.	N/A	Moderate	High
Account Management| Inactivity Logout				
AC-2.5	The Maryland Agency must require that user's sessions automatically **logout after 15 minutes of inactivity has been reached**.	Low	Moderate	High

Account Management/Usage Conditions				
AC-2.11	The Maryland Agency must ensure that the information system enforces organization-defined circumstances and/or usage conditions for organization-defined information system accounts. The Maryland Agency must describe the specific conditions or circumstances under which information system accounts can be used, for example, by restricting usage to certain days of the week, time of day, or specific durations of time. The Maryland Agency must ensure to notify administrators, suspend, or delete accounts when users are terminated, transferred, or information system usage or need-to-know/need-to-share changes. **NOTE:** This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Account Management| Account Monitoring/Atypical Use				
AC-2.12	The Maryland Agency must: ● Monitor information system accounts for atypical use, such as accessing information systems at certain times of the day and from locations that are not consistent with the normal usage patterns of individuals working in organizations ● Report atypical usage of information system accounts to DoIT designated personnel. **NOTE:** This enhancement only applies to High categorization systems. If any High systems are introduced in the future requirements will be further defined.	N/A	N/A	High

Account Management| Disable Accounts for High-Risk Individuals				
AC-2.13	The Maryland Agency must disable accounts of users posing a significant risk immediately after discovery of the risk. **NOTE:** This enhancement only applies to High categorization systems. If any High systems are introduced in the future requirements will be further defined.	N/A	N/A	High
Access Enforcement				
AC-3	The Maryland Agency must ensure that all information systems enforce assigned authorizations for logical access to the information system, that all default manufacturer passwords are changed, and that only authorized personnel are given access to the stored configuration files.	Low	Moderate	High
Information Flow Enforcement				
AC-4	The Maryland Agency must ensure that information systems enforce approved authorizations for controlling the flow of information within the system and between interconnected systems, such as boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message-filtering capability based on content. These configuration settings should be reviewed **at least annually.** Flow control restrictions include, for example: ● keeping export-controlled information from being transmitted in the clear to the Internet ● blocking outside traffic that claims to be from within the organization ● Ensure that all device management sessions come from authorized Internet Protocol (IP) addresses / subnets from the internal network ● limiting information transfers between organizations based on data structures and content	N/A	Moderate	High

Separation of Duties				
AC-5	All Maryland information systems must: a. Separate duties of individuals as necessary to prevent malevolent activity without conclusion b. Document separation of duties c. Define information system access authorizations to support separation of duties d. Utilize assigned access authorizations for UNIX systems e. Effectively segregate duties between the administration functions and the auditing functions of database system f. Have separate Administrator accounts for system and network administrators who require specific, elevated privileges to perform their job functions. More details on that separation below: The following four (4) categories of "duty" must be kept separate or compensating controls put in place to monitor activity closely: 1. IT Administration or operation (assuring systems function, to serve the system users) 2. IT Access Management (account creation, modification, removal, etc.) 3. IT Security (assuring adequacy of system controls for availability, integrity, and confidentiality) 4. IT Management (allocating adequate resources for implementation of effective IT Security Programs and system controls)	N/A	Moderate	High

Least Privilege				
AC-6	Maryland information systems must employ the concept of least privilege, allowing only authorized access for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with the Maryland Agency missions and business functions. The Maryland Agency must validate and inventory all privileged accounts; number of privileged accounts should be minimized; functions that can be performed when using privileged accounts should be limited including privileged functions that can be performed using remote access; duration that privileged users can be logged in should be limited; and privileged user activities must be logged and logs need to be reviewed regularly.	N/A	Moderate	High
Least Privilege| Authorize Access to Security Functions				
AC-6.1	Access to establish system accounts, configure access authorizations (e.g., permissions, privileges), set events to be audited, and set intrusion detection parameters must be explicitly authorized.	N/A	Moderate	High
Least Privilege| Non-Privileged Access for Non-Security Functions				
AC-6.2	Users of information system accounts, or roles, with access to establish system accounts, configure access authorizations (e.g., permissions, privileges), set events to be audited, and set intrusion detection parameters must use non-privileged accounts, or roles, when accessing other system functions, and use of privileged accounts must be audited for such functions.	N/A	Moderate	High
Least Privilege| Network Access to Privileged Commands				
AC-6.3	The Maryland Agency must authorize network access to defined privileged commands only for defined compelling operational needs and documents the rationale for such access in the security plan for the information system. This enhancement only applies to High categorization systems. If any High systems are introduced in the future requirements will be further defined.	N/A	N/A	High

Least Privilege| Privileged Accounts				
AC-6.5	The Maryland Agency must restrict privileged accounts on the information system to system administrators. Personnel who no longer require this level of access should be promptly removed from the approved access list.	N/A	Moderate	High
Least Privilege| Auditing Use of Privileged Functions				
AC-6.9	Maryland information systems must audit the execution of privileged functions. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat.	N/A	Moderate	High
Least Privilege| Prohibit non-Privileged Users from Executing Privileged Functions				
AC-6.10	Maryland information systems must prevent non-privileged users from executing privileged functions to include: ● Disabling, circumventing, or altering implemented security safeguards/countermeasures ● Create, modify and delete user accounts and groups ● Grant, modify, and remove file or database permissions ● Configure password and account lockout policy ● Configure policy regarding the number and length of sessions ● Change passwords or certificates of users other than oneself ● Determine how the application will respond to error conditions ● Determine auditable events and related parameters ● Establish log sizes, fill thresholds, and fill behavior (e.g., what happens when the log is full)	N/A	Moderate	High

Unsuccessful Login Attempts				
AC-7	Maryland information systems accounts must: a. Enforce a limit of **three (3)** consecutive invalid login attempts by a user during a **120-minute time period**; and b. Automatically lock the account for a minimum of **15 minutes** or lock the account/node until released by an administrator or other authorized account management personnel when the maximum number of unsuccessful attempts is exceeded. This control applies regardless of whether the login occurs via a local or network connection. c. UNIX systems should ensure that the login delay between login prompts **after a failed login is set to 4 seconds or greater**.	Low	Moderate	High

System Use Notification				
AC-8	All Maryland information systems must: Display an approved system use notification message or banner before granting access to the system that provides privacy and security notice consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: a. (i) the user is accessing a Maryland state information system, which may contain US government information; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized system use is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording. b. Retain the notification message or banner on the screen until the user takes explicit actions to log on to or further access the information system. c. For publicly accessible systems: (i) display the system use information when appropriate, before granting further access; (ii) display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) include a description of the authorized uses of the system in the notice given to the public users of the information system. Warning banners are displayed when individuals log in to the information system. System use notification is for information system access that includes an interactive login interface with a human user and does not require notification when an interactive interface does not exist. The following is the official DoIT warning banner: **"WARNING! THIS SYSTEM MAY CONTAIN U.S. GOVERNMENT INFORMATION, WHICH IS RESTRICTED TO AUTHORIZED USERS ONLY. UNAUTHORIZED ACCESS, USE, MISUSE, OR MODIFICATION OF THIS COMPUTER SYSTEM OR OF THE DATA CONTAINED HEREIN OR IN TRANSIT TO/FROM THIS SYSTEM CONSTITUTES A VIOLATION**	Low	Moderate	High

	OF ARTICLE 27 §§ 45A AND 146 OF THE ANNOTATED codes OF MARYLAND, TITLE 18, USC, § 1030, AND MAY SUBJECT THE INDIVIDUAL TO CRIMINAL AND CIVIL PENALTIES PURSUANT TO TITLE 26, USC, §§ 7213(A), 7213A, AND 7431. THIS SYSTEM AND EQUIPMENT ARE SUBJECT TO MONITORING TO ENSURE PROPER PERFORMANCE OF APPLICABLE SECURITY FEATURES OR PROCEDURES. SUCH MONITORING MAY RESULT IN THE ACQUISITION, RECORDING AND ANALYSIS OF ALL DATA BEING COMMUNICATED, TRANSMITTED, PROCESSED OR STORED IN THIS SYSTEM BY A USER. IF MONITORING REVEALS POSSIBLE EVIDENCE OF CRIMINAL ACTIVITY, SUCH EVIDENCE MAY BE PROVIDED TO LAW ENFORCEMENT PERSONNEL. ANYONE USING THIS SYSTEM EXPRESSLY CONSENTS TO SUCH MONITORING." Any deviation from this official banner should be approved by DoIT.			
Concurrent Session Control				
AC-10	Maryland information systems must limit the number of concurrent sessions for each system account to a maximum of **5 sessions**. Concurrent sessions must be kept to as low as possible based on risk.	N/A	Moderate	High
Session Lock				
AC-11	Maryland information systems must: a. Prevent further access to the system by initiating a session lock after **15 minutes** of inactivity or upon receiving a request from a user. b. Retain the session lock until the user reestablishes access using established identification and authentication procedures. c. Applications must manually and automatically log the user off. “Inactivity” is defined as only those actions which would require interaction of a user (e.g., system and application calls are not included).	N/A	Moderate	High

Session Lock| Pattern Hiding Displays				
AC-11.1	Maryland information systems must conceal, via the session lock, information previously visible on the display with a publicly viewable image.	N/A	Moderate	High
Session Termination				
AC-12	The Maryland Agency must terminate a user session as a targeted response to major security incidents. For authenticated sessions of public users on public-facing systems that provide access to sensitive data, Maryland information systems must terminate user sessions after no longer than **15 minutes of inactivity**. "Inactivity" is defined as only those actions which would require interaction of a user (e.g., system and application calls are not included). COTs or Custom applications are required to terminate network connections at the end of a session or due to inactivity. **NOTE:** The SSP must address variations from this guideline and applicable mitigation (if appropriate) when there are cases of anonymous access, functional and operational limitations, availability requirements and non-sensitive access.	N/A	Moderate	High

Permitted Actions without Identification or Authentication				
AC-14	Maryland information systems must: a. Identify systems and system actions that can be performed on the information system without identification and authentication consistent with the Agency mission/business function must be documented. Access to state public information can be accessed without identification or authentication. If an information system requires a system or information to be available without identification and authentication, the information system must provide rationale and seek approval. b. All information systems with public information must document in the security plan the use of public information. All information systems which require additional systems to allow access without identification or authentication must document, in the security plan, the approval and supporting rationale for why the system does not require identification and authentication.	Low	Moderate	High
Remote Access				
AC-17	The Maryland Agency must ensure that: a. Usage restrictions, configuration/connection requirements and implementation guidance for each type of allowed remote access method are established and documented. b. Remote access to information systems is authorized prior to allowing such connections. c. Multi-factor authentication mechanisms are employed for all remote access to the network. d. When administrative actions are performed from external connections, the use of an encrypted VPN connection is required.	Low	Moderate	High
Remote Access| Automated Monitoring/Control				
AC-17.1	Automated mechanisms must be employed to facilitate the monitoring and control of remote access methods, especially in cloud environments, for connectivity for unauthorized use.	N/A	Moderate	High

Remote Access| Protection of Confidentiality/Integrity Using Encryption				
AC-17.2	Cryptographic mechanisms must be used to protect the confidentiality and integrity of remote access sessions.	N/A	Moderate	High
Remote Access| Managed Access Control Points				
AC-17.3	All remote access must be controlled through a limited number of managed access points.	N/A	Moderate	High
Remote Access| Privileged Commands/ Access				
AC-17.4	Execution of privileged commands and access to security-relevant information via remote access must be authorized only for compelling operational needs and the rationale for such access must be documented in the security plans of information systems.	Low	Moderate	High
Wireless Access				
AC-18	Agencies must implement wireless connectivity using security algorithms, encryption, and features that are considered generally secure, including: a. AES encryption to secure wireless data in transit. b. Connectivity to wireless networks must be secured with protocols that support mutual-authentication, such as EAP-TLS. c. Management connectivity to the wireless infrastructure should be segregated from user connectivity. d. Physical or logical separation between guest/public networks and employee/secure networks. e. Event logging to a centralized log management server.	Low	Moderate	High
Wireless Access| Authentication and Encryption				
AC-18.1	The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.	N/A	Moderate	High

Wireless Access| Restrict Configuration by Users				
AC-18.4	The Maryland Agency must identify and explicitly authorize the users allowed to independently configure wireless networking capabilities. DoIT must ensure that users cannot independently configure wireless networking capabilities. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Wireless Access| Antennas/Transmission Power Levels				
AC-18.5	The Maryland Agency must select radio antennas and calibrate transmission power levels to reduce the probability that usable signals can be received outside of organization- controlled boundaries. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Access Control for Mobile Devices				
AC-19	Not Applicable to the current DoIT environment.	Low	Moderate	High
Access Control for Mobile Devices| Full Device/Container-Based Encryption				
AC-19.5	The Maryland Agency must **employ full-device encryption (FIPS 140-2)** to protect the confidentiality and integrity of information on mobile devices including laptops, tablets, smart phones, etc.	N/A	Moderate	High

Use of External Information Systems				
AC-20	The Maryland Agency must establish terms and conditions for all external information systems, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: a. Access the information system from external information systems. b. Process, store, or transmit organization-controlled information using external information systems. External information systems include, but are not limited to: (i) personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); (iii) information systems owned or controlled by nonfederal governmental organizations; and (iv) federal information systems that are not owned by, operated by, or under the direct supervision and authority of the organization.	Low	Moderate	High
Use of External Information Systems| Limits on Authorized Use				
AC- 20.1	The Maryland Agency must ensure that only permitted authorized individuals use an external information system to access the information system or to process, store, or transmit organization-controlled information only when: a. The implementation of required security controls on the external system as specified in the organization's information security policy and security plan is verified. b. Approved information system connection or processing agreements with the organizational entity hosting the external information system are retained.	N/A	Moderate	High

Use of External Information Systems| Portable Storage Devices				
AC-20.2	The Maryland Agency must, by policy, restrict the use and connection of portable storage devices on state information systems to those with a business need, and require any storage media containing information identified as sensitive by the data owner to be encrypted, and at all times be stored securely, until such time as the storage media has been sanitized in a manner consistent with the classification of the data.	N/A	Moderate	High
Information Sharing				
AC-21	The Maryland Agency must: a. Facilitate information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for contract sensitive information, PII, privileged medical information, or proprietary information as contractually obligated. b. Employ manual processes to assist users in making information sharing/collaboration decisions. All requirements, constraints, and information sharing circumstances should be clearly identified and documented as part of the DoIT contracts, SLAs, ISAs, or MOUs.	N/A	Moderate	High

Publicly Accessible Content				
AC-22	The Maryland Agency must ensure that: a. Individuals are designated to post information onto Maryland information systems that is publicly accessible. b. Authorized individuals are trained to ensure that publicly accessible information does not contain nonpublic information. c. Proposed content of publicly accessible information for nonpublic information is reviewed prior to posting on Maryland information systems to ensure that nonpublic information is not included. d. The content on publicly accessible Maryland information systems is reviewed for nonpublic information **prior to posting** and **at least quarterly**; and nonpublic information is removed from publicly accessible Maryland information systems, if discovered.	Low	Moderate	High

Audit and Accountability Control Requirements

Audit trails maintain a record of system activity by system or application processes and by user activity and processes. In conjunction with appropriate tools and procedures, audit trails can provide individual accountability, means to reconstruct events, detect intrusions, and identify problems. System audit trails, or event logs, provide a record of events in support of activities to monitor and enforce the IT system security policy.

All audit logs are subject to recording and routine review by the DoIT CISO, DoIT security groups, and auditors for inappropriate or illegal activity. System owners must ensure the protection of system event logs with file- level permissions, separation of duties, and all other safeguards commensurate with the highest level of sensitivity of the information residing on the system for which the logs record data. The following table outlines the minimum DoIT security control requirements which all Maryland information systems must adhere to in order to operate in a production environment.

Security Control ID	Audit and Accountability Policy and Procedures	Security Baselines		
AU-1	Maryland Agencies must develop and implement an Audit and Accountability (AU) Policy/Procedure that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance as they pertain risk assessment activities within the organization. The policy/procedure must also describe how the Maryland Agency intends to implement the security requirements associated to this NIST control family. The Audit and Accountability Policy/Procedure must be approved by the Maryland Agency's designated Senior Executive or Authorizing Official. The Audit and Accountability Policy/Procedure must be disseminated to all state and contractor personnel with IT security responsibilities within the Maryland Agency. **The policy must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**	Low	Moderate	High

Audit Events				
AU-2	The Maryland Agency must ensure that: a. Information systems audit the following events: 1. System and audit function startup and shutdown 2. Loading and unloading of services (only applicable to operating systems) 3. Installation and removal of software (only applicable to operating systems) 4. System alerts and error messages 5. All identification and authentication attempts, including change of password 6. User logon and logoff (Successful, Unsuccessful) and authorization attempts 7. System administration actions, connections, request, activities, modification of privileges, switching accounts, running privileged actions from another account, and access controls 8. All changes to logical access control authorities 9. All system changes with the potential to compromise the integrity of security policy configurations and audit log files 10. The creation, modification and deletion of objects including files, directories and user accounts 11. The creation, modification and deletion of user accounts and group accounts including super-user groups 12. The creation, modification and deletion of user account and group account privileges 13. Remote access from outside of the corporate network communication channels (e.g., modems, dedicated VPN) and all dial-in access to the system 14. All system and data interactions concerning FTI, PII, PHI, and any other sensitive data 15. All direct modifications to critical production database tables (the critical database tables are defined within the respective system security plan) by privileged users.	Low	Moderate	High

	16. These requirements are in addition to any audit events that must be captured to address any specific risks identified and support mission/business needs. b. Security audit function is coordinated with other DoIT entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events. c. A rationale for why the list of auditable events are deemed adequate to support after-the-fact investigations of security incidents is documented. d. Based on current threat information and ongoing assessment of risk, a determination is made that all events defined in AU-2(a) should be audited on a regular real-time basis. Any deviations from the list due to system audit functionality capabilities, along with justifications, must be documented in the relevant system security plans. e. Validate that the cloud provider protects audit log data from modification and restricted to personnel required to have access.			
Audit Events | Reviews and Updates				
AU-2.3	The Agency must review the list of auditable events for information systems **annually**. The Agency CISO reviews and updates the minimum list of auditable events **annually**.	N/A	Moderate	High

Content of Audit Records				
AU-3	The Maryland information systems must generate audit records that contain sufficient information to establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. At a minimum, all events should contain the following: ● Event type ● Service timestamps and/or log date and time ● Location of the event ● User ID (if available), but do not log password used ● Action/request attempted (particularly: interface status changes, changes to the system configuration, access list matches and/or failures) ● Success or failure of the action (the outcome of the event) ● Date/time stamp of the event and Source address (Hostname or IP) of the request ● The component of the information system (e.g., software component, a hardware component) where the event occurred ● Disabling of audit features or failures ● Clearing of audit log files	Low	Moderate	High
Content of Audit Records| Additional Audit Information				
AU-3.1	The Maryland Agency must ensure that information systems include additional detailed information in the audit records when system functionality permits. Example of additional information may be full text recording of privileged commands or the individual identities of group account users, etc.	N/A	Moderate	High

Content of Audit Records | Centralized Management of Planned Audit Record Content				
AU-3.2	Maryland information systems must provide centralized management and configuration of the content to be captured in audit records generated by the central logging system. This enhancement only applies to High categorization systems. If any High systems are introduced in the future these requirements will be further defined.	N/A	N/A	High
Audit Storage Capacity				
AU-4	The Maryland Agency must ensure that sufficient audit record storage capacity is allocated for information systems to prevent log files from filling up between log rotation intervals. The Maryland Agency must also define and document the storage capacity limit for audit logs and ensure mechanisms are in place to alert when a storage device nears capacity. In addition, ensure that audit logs are backed up, archived off of the system, and retained for a period of **7 years**.	Low	Moderate	High

Response to Audit Processing Failure				
AU-5	The Maryland Agency must ensure that, in the event of an audit processing failure, information systems: a. Alert designated Agency officials in the event of an audit failure, any unusual or inappropriate activity, or audit storage capacity being reached. b. Monitor system operational status using operating system or system audit logs and verify functions and performance of the system. **Either shut down, overwrite the oldest audit records** or cease information system processing, depending on system data availability and integrity requirements. It is required that a justification and selection be documented in the system security plan (SSP). c. Provide a warning when allocated audit record storage volume reaches a maximum audit record storage capacity.	Low	Moderate	High
Response to Audit Processing Failures | Audit Storage Capacity				
AU-5.1	Information systems must provide a warning to authorized personnel (administrators) when allocated audit record storage volume **reaches 90%** of maximum audit record storage capacity. This enhancement only applies to High categorization systems. If any High systems are introduced in the future these requirements will be further defined.	N/A	N/A	High
Response to Audit Processing Failures | Real-Time Alerts				
AU-5.2	Information systems must provide a real-time alert to system administrators when the audit storage capacity **reaches 90%**; when there is a failure in audit capturing mechanism; or when any other event occurs that would cause audit processes to fail. This enhancement only applies to High categorization systems. If any High systems are introduced in the future these requirements will be further defined.	N/A	N/A	High

Audit Review, Analysis and Reporting				
AU-6	The Maryland Agency must ensure that: a. Audit records for information systems are reviewed and analyzed in **near real time** or at **minimum weekly** for indications of inappropriate or unusual activity. Inappropriate or unusual activities should be defined in the SSP for each system. b. Any findings are documented and reported to DoIT designated officials including incident response team, and if necessary findings are escalated to CISO. All information systems connected to a state network should utilize the DoIT -approved centralized audit record management solution with the requirements defined by the CISO and the program manager for the enterprise-wide auditing solution. Any deviations due to the functionality, operational requirements, or capabilities of a system which is not utilizing the central logging system for audit review, analysis, and reporting process, must be clearly defined and justified in the system security plan. Compensating security controls should be clearly documented to meet security control requirements.	Low	Moderate	High
Audit Review, Analysis, and Reporting | Processing Integration				
AU-6.1	Information systems should integrate automated mechanisms for audit review, analysis, and reporting processes to support DoIT processes for investigation and response to suspicious activities.	N/A	Moderate	High
Audit Review, Analysis, and Reporting | Correlate Audit Repositories				
AU-6.3	The Maryland Agency must ensure that information system audit records are analyzed and correlated across different repositories to gain organization-wide situational awareness.	N/A	Moderate	High

Audit Review, Analysis, and Reporting | Integration/ Scanning and Monitoring Capabilities				
AU-6.5	The Maryland Agency must integrate analysis of audit records with analysis of vulnerability scanning information and information system monitoring information to further enhance the ability to identify inappropriate or unusual activity. This enhancement only applies to High categorization systems. If any High systems are introduced in the future these requirements will be further defined.	N/A	N/A	High
Audit Review, Analysis, and Reporting| Correlation with Physical Monitoring				
AU-6.6	The Maryland Agency must correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity. This enhancement only applies to High categorization systems. If any High systems are introduced in the future these requirements will be further defined.	N/A	N/A	High
Audit Reduction and Report Generation				
AU-7	Maryland information systems must provide an audit reduction and report generation capability that: a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents. b. Does not alter the original content or time ordering of audit records. The Agency must conduct audit reviews and analysis using a centralized automated tool. **NOTE:** Any information system that does not or currently is not capable of providing logs to the DoIT enterprise audit generation tools due to system functionality and operational requirements must have documented in its system security plan the process by which its logs may be sorted and organized for more meaningful analysis.	N/A	Moderate	High

Audit Reduction and Report Generation| Automatic Processing				
AU-7.1	Information systems should provide the capability to automatically process audit records for events of interest based upon selectable event criteria. Events of interest include, for example: identities of individuals, event type, event dates, event location, IP address involved, information objects, or system resources involved, etc.	N/A	Moderate	High
Time Stamps				
AU-8	Maryland information systems must: a. Use internal system clocks to generate timestamps for audit records. b. Record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets the **less than 5 second** requirement.	Low	Moderate	High
Time Stamps| Synchronization with Authoritative Time				
AU-8.1	Maryland information systems must: a. Compare the internal information system clocks at least daily with NTP time source. b. Synchronize, if the offset is greater than 1 second, the internal system clocks to a minimum of three authenticated NTP time sources with a stratum level of 5 or higher (1-5) that maintains synchronization with NIST.	Low	Moderate	High
Protection of Audit Information				
AU-9	Maryland information systems must protect audit information and audit tools from unauthorized access, use, modification, and deletion.	Low	Moderate	High

Protection of Audit Information| Audit Backup on Separate Physical Systems/Components				
AU-9.2	Maryland information systems must back up audit records in accordance with IRS best practices, in which audit logs/tails are retained for a total of **seven (7) years**. These backups are stored onto a different system (Physically) or system component than the system or component being audited. This enhancement only applies to High categorization systems. If any High systems are introduced in the future these requirements will be further defined.	N/A	N/A	High
Protection of Audit Information| Cryptographic Protection				
AU-9.3	Maryland information systems must implement cryptographic mechanisms to protect the integrity of audit information and audit tools. This enhancement only applies to High categorization systems. If any High systems are introduced in the future these requirements will be further defined.	N/A	N/A	High

Protection of Audit Information| Access by Subset of Privileged Users				
AU-9.4	The Maryland Agency must authorize access to the management of audit functionality to only **security administrators or authorized staff** other than system and network administrators. Authorized staff must have privileged access and be assigned the responsibility for performing security audit functions. These **individuals should be documented in the SSP.** The Maryland Agency must ensure that audit trails **cannot** be read or modified by **non-administrator users**, **system and network administrators.** Individuals with privileged access to an information system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit activities or modifying audit records. Privileged access should be further defined between audit-related privileges and other privileges, thus limiting access to those users with audit-related privileges. To ensure the integrity and objectivity of the auditing and network monitoring functions, segregation of duties must be maintained. No single individual may have control over all phases of audit functionality and network monitoring.	N/A	Moderate	High
Non-Repudiation				
AU-10	Agency System Owners must ensure that information systems protect against an individual (or processes acting on behalf of an individual) falsely denying having performed an action (e.g., created information, sent message, approved information to indicate concurrence or sign a contract, or received a message). This security control only applies to High categorization systems. If any High systems are introduced in the future these requirements will be further defined.	N/A	N/A	High

Audit Record Retention				
AU-11	The Maryland Agency must ensure that audit logs are retained online for **90 days** and archived for **seven (7 years) (for the remainder of the year they were made plus six years)** to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	Low	Moderate	High
Audit Generation				
AU-12	Agencies must ensure that information systems: a. Provide audit record generation capability for the list of auditable events in AU-2 for all system components and super users. b. Allow designated DoIT personnel to select which auditable events are to be audited by specific components of the system. c. Generate audit records for the list of audited events in AU-2 with the content defined in AU-3.	Low	Moderate	High
Audit Generation| System-Wide/Time-Correlated Audit Trail				
AU-12.1	Audit records from all information system components eligible for the DoIT -approved centralized audit record management solution must be compiled into a system-wide (logical or physical) audit trail that is time-correlated to within a two-minute level of tolerance for relationships between time stamps of individual records in the audit trail. This enhancement only applies to High categorization systems. If any High systems are introduced in the future these requirements will be further defined.	N/A	N/A	High
Audit Generation| Changes by Authorized Individuals				
AU-12.3	Audit records from all information system components eligible for the DoIT -approved centralized audit record management solution must be compiled into a system-wide (logical or physical) audit trail that is time-correlated to within a two-minute level of tolerance for relationships between time stamps of individual records in the audit trail. This enhancement only applies to High categorization systems. If any High systems are introduced in the future these requirements will be further defined.	N/A	N/A	High

CROSS-ORGANIZATIONAL AUDITING				
AU-16	The Maryland Agency must capture the identity of individuals issuing requests at the initial information system, and subsequent systems record that the requests emanated from authorized individuals. DoIT also must review cross-organizational auditing information and identify anomalies across all cloud entities. **NOTE:** This control is only applicable for systems in an outsourced data center and cloud computing environments.	N/A	Moderate	High

Identification and Authorization Control Requirements

Identification and authentication is a technical measure that prevents unauthorized users (or unauthorized processes) from entering an IT system. Access control usually requires that the system be able to identify and differentiate users. All DoIT and Maryland IT systems must have a means to enforce user accountability when using state IT systems, so that system activity (both authorized and unauthorized) can be traced to specific users. To ensure user accountability, DoIT requires that all Maryland IT systems implement a method of user identification and authentication. The user identification tells the system who the users are; the authentication mechanism provides an added level of assurance that the users really are who they say they are. Authentication consists of something a user knows (such as a password), something the user has (such as a token or smart card), or something the user is (such as a fingerprint). User identification and authentication also can enforce separation of duties. The following table outlines the minimum DoIT security control requirements which all Maryland information systems must adhere to in order to operate in a production environment.

Security Control ID	Identification and Authentication Policy and Procedures	Security Baselines		
IA-1	Maryland Agencies must develop and implement an Identification and Authentication (IA) Policy/Procedure that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance as they pertain risk assessment activities within the organization. The policy/procedure must also describe how the Maryland Agency intends to implement the security requirements associated to this NIST control family. The Identification and Authentication Policy/Procedure must be approved by the Maryland Agency's designated Senior Executive or AO. The Identification and Authentication Policy/Procedure must be disseminated to all state and contractor personnel with IT security responsibilities within the Maryland Agency. **The policy must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**	Low	Moderate	High

Identification and Authentication (Organizational Users)				
IA-2	All Maryland information systems must uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users). User identification and authentication provides for accountability of user system activities and enforce separation of duties by limiting access.	Low	Moderate	High
Identification and Authentication| Network Access to Privileged Accounts				
IA-2.1	Maryland information systems should implement multifactor authentication using a DoIT approved token for network access to privileged accounts. Network access is any access to an organizational information system by a user (or process acting on behalf of a user) where such access is obtained through a network connection. The Maryland Agency must ensure additional restrictions are in place, including: a. Use of null passwords is revoked. b. Individual user accounts have been created for each authorized user. c. Groups, user accounts without passwords, or duplicate accounts should not exist. d. No shared accounts are used other than when operationally required (e.g., root accounts). e. Passwords are not displayed in clear text and must be encrypted or hashed with an industry approved standard.	Low	Moderate	High

Identification and Authentication| Network Access to Non-Privileged Accounts				
IA-2.2	Maryland information systems should implement multifactor authentication for network access to non-privileged accounts. Network access is any access to an organizational information system by a user (or process acting on behalf of a user) where such access is obtained through a network connection. **NOTE**: For cloud services, **multi-factor authentication** is required for both administrators and end users. See NIST 800-63B for additional information on multifactor authentication.	N/A	Moderate	High
Identification and Authentication| Local Access to Privileged Accounts				
IA-2.3	Maryland information systems should implement multifactor authentication for local access to privileged accounts. The use of null passwords is prohibited. Local access is any access to an organizational information system by a user (or process acting on behalf of a user) where such access is obtained by direct connection without the use of a network.	N/A	Moderate	High
Identification and Authentication| Local Access to Non-Privileged Accounts				
IA-2.4	Maryland information systems should implement multifactor authentication for local access to non-privileged accounts. The use of null passwords is prohibited. Local access is any access to an organizational information system by a user (or process acting on behalf of a user) where such access is obtained by direct connection without the use of a network. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High

Identification and Authentication| Network Access to Privileged Accounts-Replay Resistant				
IA-2.8	Maryland information systems must implement replay-resistant authentication mechanisms for network access to privileged accounts. Replay-resistant techniques include, for example, protocols that use nonce or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.	N/A	Moderate	High
Identification and Authentication| Network Access to Non-Privileged Accounts-Replay Resistant				
IA-2.9	Maryland information systems must implement replay-resistant authentication mechanisms for network access to non-privileged accounts. Replay-resistant techniques include, for example, protocols that use nonce or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Identification and Authentication| Remote Access – Separate Device				
IA-2.11	Maryland information systems must implement **multifactor authentication** for remote access to privileged and non-privileged accounts such that one of the factors is provided **using a software token** which meets current NIST 800-63 guidelines on Level 3 requirements or higher.	N/A	Moderate	High
Identification and Authentication| Acceptance of PIV Credentials				
IA-2.12	For agencies where Personal Identity Verification (PIV) credentials are issued, information systems with sensitive data must be designed to accept and electronically verify PIV credentials.	Low	Moderate	High

Device Identification and Authentication				
IA-3	The Maryland Agency must ensure that information systems uniquely identify and authenticate all endpoint devices (especially those that receive, process, store, or transmit FTI, PII, PHI or other sensitive information) to the network **before establishing a connection.**	N/A	Moderate	High
Identifier Management				
IA-4	Maryland information systems manage identifiers by: a. Receiving authorization from a designated DoIT official (supervisor, security monitor, and system administrator) to assign an individual, group, role, or device identifier. b. Selecting an identifier that identifies an individual, group, role or device. c. Assigning the identifier to the intended individual, group, role, or device. d. Preventing reuse of identifiers for **1 year**. e. Disabling identifiers after **120** days of inactivity. For cloud services, identifier management should also include; a. Selecting an identifier that uniquely identifies an individual with supplemental controls provided by the cloud provider to ensure duplicate identifiers are not stored. b. Assigning the user identifier to the intended party. c. Preventing reuse of user identifiers.	Low	Moderate	High

Authenticator Management				
IA-5	Information system authenticators must be managed (e.g., tokens, PKI certificates, passwords, and key cards) by: a. Verifying, as a part of initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator. b. Establishing initial authenticator content for authenticators defined by the DoIT. c. Ensuring that authenticators have sufficient strength of mechanism for their intended use. d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators. e. Changing default authenticators upon information system installation. f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate). g. Changing/refreshing authenticators (passwords) every **45** days (**Note:** Passwords must be changed immediately or disabled if known or suspected to be compromised). h. Protecting authenticator content from unauthorized disclosure and modification. i. Requiring users to take, and have devices implement, specific measures to safeguard authenticators. j. Changing authenticators for group/role accounts when membership to those accounts' changes. k. Service accounts which use elevated privileges, such as administrator or root, the passwords on such accounts must be changed **at least annually**. Electronic authentication methods to provide services to citizens must comply with NIST SP 800-63, *Digital Identity Guidelines.* For public facing systems that require user identification and authentication E-authentication criteria should be used	Low	Moderate	High

	to address authentication requirements along with the DoIT policy and procedures documented under this security control. Deviations from DoIT Password Management Policy must be documented and approved by the Authorizing Official. Then approval can be added to the appropriate system security documentation.			

Authenticator Management| Password Based Authentication				
IA-5.1	For password-based authentication, Maryland information systems must: 1. Enforce the following minimum password complexity requirements: a. At least twelve (12) non-blank characters; b. Characters from three (3) of the following four (4) categories: c. At least one (1) english upper-case characters (A-Z) d. At least one (1) english lower-case characters (a-z) e. At least one (1) numbers based on 10 digits (0-9) f. At least one (1) Non-Alphanumeric/special characters (ex.,!, $, #) 2. Enforce at least three (3) changed character rule when new passwords are created 3. Store and transmit only encrypted representation of passwords using FISMA compliant valid encryption as defined by NIST standards 4. Enforce a password minimum lifetime restriction of two (2) days and a maximum lifetime restriction of 90 days 5. Service account passwords may be set to never expire, but must be denied local logon, and must be identified in the system's SSP and supporting documentation for tracking. 6. Prohibit password reuse for a specific account for 24 generations or four (4) years 7. Allows the use of a temporary password for system logons with an immediate change to a permanent password 8. Password-protect system initialization (boot) settings 9. Passwords must not contain: a. Account Username b. Beginning or trailing blanks c. More than two identical characters in a row d. Recommendations for passwords include avoiding predictability and the following	Low	Moderate	High

	methods and components: e. Common words or phrases f. Typical topologies (patterns) g. Initial cap word, followed by number, followed by special character- (e.g., Fall2015!) h. Special character, number, Cap word (e.g., #1 Redskins) i. Social information j. Family names, Pet names k. Telephone numbers, SSNs, Anniversaries, or birthdays l. Address, zip code, street name Passwords used on external systems or social websites should never be used for work For public facing systems that require user identification and authentication E-authentication criteria should be used to address authentication requirements along with the DoIT policy and procedures documented under this security control.			
Authenticator Management| PKI Based Authentication				
IA-5.2	For PKI-based authentication, Maryland information systems must: a. Validate certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information. b. Enforce authorized access to the corresponding private key. c. Map the authenticated identity to the account of the individual or group. d. Implement a local cache of revocation data to support path delivery and validation in case of inability to access revocation information via the network.	N/A	Moderate	High

Authenticator Management| In Person or Trusted Third – Party Registration				
IA-5.3	The Maryland Agency must require that employees and contractors go through a registration process to receive IDs and tokens Registration process is carried out in person before a designated registration authority (The Maryland Agency Security Office) with authorization by a designated Maryland Agency official (e.g., a supervisor).	N/A	Moderate	High
Authenticator Management| Hardware Token-Based Authentication				
IA-5.11	The information system, for hardware or software token-based authentication must employ mechanisms that are assessed and approved by the Agency CISO that meets the requirements of applicable state and federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	Low	Moderate	High
Authenticator Feedback				
IA-6	All Maryland information systems must obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	Low	Moderate	High
Cryptographic Module Authentication				
IA-7	Maryland information systems must implement mechanisms (ssh v2, TLS 1.2 or above, and 128-bit key lengths) for authentication to a cryptographic module that meets the requirements of FIPS 140-2 and/or applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.	Low	Moderate	High

Identification and Authentication (Non-Organizational Users)				
IA-8	Maryland information systems must uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users). Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization. Multi-factor authentication is utilized for all remote network access to privileged and non-privileged accounts for information systems that receive, process, store or transmit sensitive information.	Low	Moderate	High
Identification and Authentication| Acceptance of PIV Credentials From Other Agencies				
IA-8.1	Maryland information systems should accept and electronically verify Personal Identity Verification (PIV) credentials from other federal and state agencies as applicable.	Low	Moderate	High
Identification and Authentication| Acceptance of Third- Party Credentials				
IA-8.2	The Maryland Agency public facing websites should accept only FICAM -approved third-party credentials as applicable. Third-party credentials are those credentials issued by nonfederal government entities approved by the Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative.	Low	Moderate	High
Identification and Authentication| Use of FICAM Approved Products				
IA-8.3	The Maryland Agency employs only FICAM-approved information system components in the Maryland Agency designed information system to accept third-party credentials as applicable. This control enhancement typically applies to information systems that are accessible to the general public, for example, public-facing websites.	Low	Moderate	High

Identification and Authentication| Use of FICAM Issued Profiles				
IA-8.4	Maryland information systems should conform to FICAM-issued profiles as applicable.	Low	Moderate	High

System and Communications Control Requirements

The System and Communications Protection control family describes the technical mechanisms that an organization can employ to provide a baseline defense against basic system and communication attack methods. Most of the control mechanisms are designed to be implemented at the server and network tier of the enterprise computing environment; however, selected controls may apply to enterprise applications as well. Common themes, including segmenting computing resources and applying data encryption characterize the system and communications protection control family. The following table outlines the minimum DoIT security control requirements which all Maryland information systems must adhere to in order to operate in a production environment.

Security Control ID	System and Communication Protection (SC) Policy and Procedures	Security Baselines		
SC-1	Maryland Agencies must develop and implement a System and Communication Protection (SC) Policy/Procedure that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance as they pertain risk assessment activities within the organization. The policy/procedure must also describe how the Maryland Agency intends to implement the security requirements associated to this NIST control family. The System and Communication Protection Policy/Procedure must be approved by the Maryland Agency's designated Senior Executive or Authorizing Official. The System and Communication Protection Policy/Procedure must be disseminated to all state and contractor personnel with IT security responsibilities within the Maryland Agency. **The policy must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**	Low	Moderate	High

Application Partitioning				
SC-2	Maryland information systems must either logically or physically separate user functionality (including user interface services) from information system management functionality. Separation may be accomplished using the following examples, but not limited to; ● Different computers ● Different central processing units ● Different instances of the operating system ● Different network addresses	N/A	Moderate	High
Security Function Isolation				
SC-3	Maryland information systems should isolate security functions from non-security functions. This control only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Information in Shared Resources				
SC-4	The Maryland Agency must ensure that information systems prevent unauthorized and unintended information transfer via shared system resources by properly removing data remnants. See NIST SP 800-66 and SP 800-88 for additional details.	N/A	Moderate	High

Denial of Service Protection				
SC-5	The Maryland Agency must ensure that information systems protect against or limit the effect of denial of service attacks including directed malicious attacks against DoIT network, system, or services by employing adequate boundary protection devices which could thwart basic types of attacks such as: ● Tear-drop ● SYN flood ● Smurf (ICMP) flood ● Ping flood ● Domain Name System (DNS) Server Denial of Service (DoS) ● Worm and Distributed Denial of Service (DDoS) Agent Infestation ● Any updated type of attack identified by US-CERT Boundary protections are to include countermeasures for DoS attacks listed above to prevent or limit the impact of any such attack. Countermeasures should include; ● Monitoring and controlling the total number of user sessions opened ● The total number of concurrent sessions that can be opened by a single user ● The total amount of idle time (15 minutes) before the user session is forced to terminate. ● System limitation for the number of concurrent VPN sessions that can be opened by a single user to **one (1)**. The details of these requirements, specific configuration settings, and manual checks can be found on the Office of Safeguards website.	Low	Moderate	High

Boundary Protection				
SC-7	The Maryland Agency must ensure that information systems: a. Monitor and control communications at the external boundaries of information systems and at key internal boundaries within information systems. b. Employ NAT to protect internal IPs from being publicly disclosed. c. Publicly accessible components reside in a screened subnet (DMZ) architecture. d. Implement sub networks for publicly accessible system components that are physically and logically separated from the network. e. Maintain an access control list restricting traffic from known malicious IP addresses. f. Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices.	Low	Moderate	High
Boundary Protection| Access Points				
SC-7.3	The Maryland Agency must ensure the number of access points to information systems are limited to allow for better monitoring of inbound and outbound communications and network traffic.	N/A	Moderate	High

Boundary Protection| External Telecommunications Services				
SC-7.4	The Maryland Agency must ensure that: a. A managed interface (boundary protection devices in an effective security architecture) is implemented for each external telecommunication service. b. A traffic flow policy is established for each managed interface. c. Security controls are employed as needed to protect the confidentiality and integrity of information being transmitted across each interface. d. Each exception to the traffic flow policy is documented with a supporting mission/business needs and duration of that need. e. Exceptions to the traffic flow policy are reviewed **quarterly**; and exceptions that are no longer supported by an explicit mission/ business needs are removed.	N/A	Moderate	High
Boundary Protection| Deny by Default/Allow by Exception				
SC-7.5	Information systems must, at managed interfaces, deny network communication traffic by default and allow network communication traffic by exception (e.g., deny all, permit by exception). The Maryland Agency manually and/or automatically updates the exception list through a product vendor and/or managed service at least quarterly.	N/A	Moderate	High
Boundary Protection| Prevent Split Tunneling for Remote Devices				
SC-7.7	Maryland information systems must, in conjunction with a remote device, prevent the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.	N/A	Moderate	High

Boundary Protection| Route Traffic to Authenticated Proxy Servers				
SC-7.8	Information systems must route IT traffic destined for the system or application and all external networks through authenticated proxy servers within the managed interfaces of boundary protection devices. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Boundary Protection| Fail Secure				
SC-7.18	Maryland information systems must fail securely in the event of an operational failure of a boundary protection device. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High
Boundary Protection| Isolation of Information System Components				
SC-7.21	The Maryland Agency must employ boundary protection mechanisms to separate organization-defined information system components both, physically and logically that support different organization-defined missions and/or business functions.	N/A	Moderate	High
Transmission Confidentiality and Integrity				
SC-8	Maryland information systems must protect the confidentiality and integrity of both internally and externally transmitted information to prevent unauthorized disclosure of data and FTI and detect changes to information during transmission across the wide area network (WAN) and within the local area network (LAN) as appropriate. DoIT uses Federal Information Processing Standard (FIPS) 140-2 validated encryption with a minimum version of Secure Shell (SSH) version 2 and Transport Layer Security (TLS) 1.2.	N/A	Moderate	High

Transmission Confidentiality and Integrity| Cryptographic or Alternate Physical Protection				
SC-8.1	Cryptographic mechanisms must be implemented to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by alternative physical safeguards (e.g., protective distribution systems).	N/A	Moderate	High
Network Disconnect				
SC-10	Maryland information systems are to terminate network connections at the end of a session **or after 30 minutes of inactivity.**	N/A	Moderate	High
Cryptographic Key Establishment and Management				
SC-12	The Maryland Agency must ensure that cryptographic keys for required cryptography employed within the information system, are established and managed by: a. Establishing manual procedures or automated mechanisms for digital certificate generation, installation, and distribution. b. Generating and storing subscriber key pairs using FIPS 140-2 validated cryptographic modules. c. Prohibiting the use of the same public/private key pairs for encryption and digital signatures. d. Protecting private keys using strong, complex passwords, which are in line with DoIT's Password policy. e. Revoking certificates if the associated private key is compromised; management requests revocation; or the certificate is no longer needed. These key management requirements are in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance including current NIST SP 800 133 and FIPS 140-2.	Low	Moderate	High
Cryptographic Key Establishment and Management| Availability				
SC-12.1	Availability of information must be maintained in the event of the loss of cryptographic keys by users. This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High

Cryptographic Protection				
SC-13	When cryptography is employed within information systems, the System Owner must ensure the information system implements cryptographic mechanisms that comply with applicable federal laws, Executive Orders, directives, policies, regulations and standards. The Maryland Agency must employ FIPs-140-2 compliant cryptographic modules to protect sensitive data to include, but not limited to, PII information, provision of digital signatures, etc. Applicable federal standards for employing cryptography in non-national security information systems are documented in the FIPS documents and NIST Special Publications. Use of cryptographic modules must comply with NIST documented standards including timeline for deprecation. New purchases and amendments (e.g., additional licenses, cryptographic upgrade) to existing cryptographic modules must be FISMA compliant as per NIST documentation. **NOTE:** NIST Special Publications have pointed out potential flaws in the development of standards by which encryption hardware and modules have been certified under the FIPS 140-2 certification program (e.g., modules that use Triple Data Encryption Algorithm). When there is a conflict, the standards that are documented in the NIST Special Publications take precedent.	Low	Moderate	High

Collaborative Computing Devices				
SC-15	The Maryland Agency must ensure information systems: a. Prohibit remote activation of collaborative computing devices (e.g., including networked white boards, cameras, and microphones) with the exceptions identified in the System and Communication Protection Procedures. b. Provide an explicit indication of use to users physically present at the device (e.g., signals that indicate that collaborative computing devices are activated). **NOTE:** Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.	Low	Moderate	High
Public Key Infrastructure Certificates				
SC-17	The Maryland Agency must ensure that public key certificates are issued by an internal CA that governs the operation of the Public Key Infrastructure (PKI) consisting of products and services that provide and manage X.509 certificates for public-key cryptography or obtains public key certificates from an approved service provider. The Maryland Agency must also manage the information system trust stores to ensure only approved trust anchors are in the trust stores.	N/A	Moderate	High
Mobile Code				
SC-18	The Maryland Agency must ensure that: a. Acceptable and unacceptable mobile code and mobile code technologies are defined. b. Usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies are established. c. The use of mobile code within the information systems is authorized, monitored and controlled. Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, and VBScript. For specific details on the mobile code requirements, see NIST SP 800-28	N/A	Moderate	High

Voice Over Internet Protocol (VoIP)				
SC-19	The Maryland Agency must ensure that: a. Usage restrictions and implementation guidance are established for VoIP technologies based on the potential to cause damage to the information system if used maliciously. b. The use of VoIP within the information systems is authorized, monitored and controlled.	N/A	Moderate	High
Secure Name/Address Resolution Service (Authoritative Source)				
SC-20	Maryland information systems must: a. Provide additional data origin and integrity artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries. b. 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. This control enables remote clients to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service. Digital signatures and cryptographic keys are examples of additional artifacts. DNS resource records are examples of authoritative data. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data.	Low	Moderate	High
Secure Name/Address Resolution Service (Recursive or Caching Resolver)				
SC-21	Maryland information systems must request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.	Low	Moderate	High

Architecture and Provisioning for Name/Address Resolution Service				
SC-22	The Maryland Agency must ensure information systems that collectively provide name/address resolution service for the DoIT are fault tolerant and implement internal/external role separation.	Low	Moderate	High
Session Authenticity				
SC-23	The Maryland Agency must ensure information systems provide mechanisms to protect the authenticity of communications sessions. This control addresses communications protection at the session, versus packet level (e.g., sessions in service- oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes, for example, protecting against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions.	N/A	Moderate	High
Fail in Known State				
SC-24	The Maryland Agency must ensure that information systems fail to a known secure state for kernel-based or whole system failures preserving pre-defined configuration settings in failure. This control only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.	N/A	N/A	High

Protection of Information at Rest				
SC-28	Maryland information systems must protect the confidentiality and integrity of configuration and/or rule sets for firewalls, gateway, intrusion detection/prevention systems, authenticator content, databases maintaining sensitive PII information or other sensitive data and FTI at rest on a storage device or on a secondary storage device like a tape drive using FIPS 140-2 cryptographic mechanisms.	N/A	Moderate	High
Process Isolation				
SC-39	Maryland information systems will maintain a separate execution domain for each executing process. 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.	Low	Moderate	High

Privacy Controls

The privacy controls facilitate DoIT ’s efforts to comply with the privacy requirements affecting those organizational programs and systems that collect, use, maintain, share, or dispose of personally identifiable information (PII) or other activities that raise privacy risks.

The privacy controls listed in this IT Security Manual are primarily for use by an organization’s Senior Chief Privacy Officer (CPO) when working with program managers, mission/business owners, information owners, CIO, CISO, information system developers/integrators, and risk executives to determine how best to incorporate effective privacy protections and practices (e.g., privacy controls) within DoIT programs and information systems and the environments in which they operate. Agencies working with data governed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) should already have a CPO in place. Those agencies that do not have a CPO should look to appoint one as Agencies develop and improve their privacy program.

Maryland information systems (MIS) should analyze and apply each privacy control with respect to distinct mission/business and operational needs based on legal authorities and obligations. This will enable individual agencies and DoIT to determine the information practices that are compliant with law and policy and those that may need review. It also enables agencies to tailor the privacy controls to meet their defined and specific needs at the organization level, mission/business process level, and information system level.

Documented privacy control enhancements reflect best practices which MIS should strive to achieve but are not mandatory. DoIT and Maryland should decide when to apply control enhancements to support organizations particular missions/business functions.

Authority and Purpose

This family must ensure identification of the legal basis that authorizes collection of PII or activity which may impact privacy. Furthermore, this control family outlines the purpose(s) for which the data is being collected. The following table outlines the minimum DoIT security control requirements which all Maryland information systems must adhere to in order to operate in a production environment.

Security Control ID	Authority to Collect	Security Baselines		
AP-1	The Maryland Agency must determine and document its legal authority to collect, use, maintain, and share PII, either generally or in support of a specific program or information system requirement The policy must be reviewed and updated **at least every 3 years** and the procedures reviewed and updated **at least annually**.	Low	Moderate	High
Purpose Specification				
AP-2	The Maryland Agency must describe in its privacy notices the purpose(s) for which PII is collected, used, maintained, and shared.	N/A	Moderate	High

Accountability, Audit, and Risk Management

The privacy controls below provide an overview of the governance, monitoring, risk management, and assessment used within the state. Implementing these controls demonstrates compliance with applicable privacy protection requirements and minimize the overall risk to managing privacy. The following table outlines the minimum DoIT security control requirements which all Maryland information systems must adhere to in order to operate in a production environment.

Security Control ID	Governance and Privacy Program	Security Baselines		
AR-1	The Maryland Agency must establish a Privacy Program consistent with NIST Special Publication 800-53 (current revision) requirements. https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final The Maryland Agency privacy policy must be reviewed and updated **at least every 3 years** and the procedures reviewed and updated **at least annually**.	Low	Moderate	High
Privacy Impact and Risk Assessment				
AR-2	The Maryland Agency must: a. Document and implement a privacy risk management process that assesses privacy risk to individuals resulting from the collection, storage, sharing, transmitting, use, and disposal of PII b. Conduct privacy impact assessments for information systems, programs, and other AE activities that pose a risk to the privacy of PII	Low	Moderate	High
Privacy Requirements for Contractors and Service Providers				
AR-3	The Maryland Agency must: a. Establish privacy roles, responsibilities, and access requirements for contractors and service providers c. Include privacy requirements in contracts and other acquisition-related documents	Low	Moderate	High

Privacy Monitoring and Auditing				
AR-4	The Maryland Agency must: a. Monitor and audit privacy controls and internal privacy policy as required to ensure effective implementation d. Where applicable, comply with CMS privacy oversight monitoring and auditing policies and procedures	Low	Moderate	High
Privacy Awareness and Training				
AR-5	The Maryland Agency must: a. Develop, implement, and update a comprehensive privacy, training and awareness strategy aimed at ensuring personnel understand privacy responsibilities and procedures e. Administer basic privacy training at least annually, and targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII at least annually DoIT personnel and contractors are required to re-certify and accept privacy training and requirements on an **annual** basis.	Low	Moderate	High
Privacy Reporting				
AR-6	N/A (Maryland state agencies are not required to provide privacy reports to federal oversight organizations)			
Privacy Enhanced System Design and Development				
AR-7	The Maryland Agency must design information systems that support privacy with automated privacy controls. DoIT recommends an additional focus on implementing the following control families to enhance privacy protection: ● Access Control (AC) ● Auditing and Accountability (AU) ● Identification and Authentication (IA) ● System and Communication Protection (SC) ● Configuration Management (CM) ● System and Information Integrity (SI)	Low	Moderate	High

Accounting of Disclosures				
AR-8	The Maryland Agency must: a. Keep an accurate accounting of disclosures of information held in each system of records under its control, including: 1. **Date**, **nature**, and **purpose** of each disclosure of a record 2. **Name** and **address** of the person or agency to which the disclosure was made b. Retain the accounting of disclosures for **the life of the record or five years** after the disclosure is made, whichever is longer c. Make the accounting of disclosures available to the person named in the record upon request.	Low	Moderate	High

Data Quality and Integrity

This control family must ensure that PII which is collected and maintained is accurate, relevant, timely, and complete for the purpose for which it is to be used. The following table outlines the minimum DoIT security control requirements which all Maryland information systems must adhere to in order to operate in a production environment.

Security Control ID	Data Quality	Security Baselines		
DI-1	The Maryland Agency must: a. Confirm to the greatest extent practicable upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that information b. Collect PII directly from the individual to the greatest extent practicable c. Check for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems as directed by the State d. Issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information The policy must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.	Low	Moderate	High
Validate PII				
DI-1 (1)	The Maryland Agency must request the individual or the individual's authorized representative to validate PII during the collection process.	Low	Moderate	High
Re-validate PII				
DI-1 (2)	The Maryland Agency must: a. Establish privacy roles, responsibilities, and access requirements for contractors and service providers f. Include privacy requirements in contracts and other acquisition-related documents	Low	Moderate	High

Data Integrity and Data Integrity Board				
DI-2	The Maryland Agency must: a. Document processes and procedures to ensure the integrity of PII through existing security controls g. Establish a Data Integrity Board when appropriate to oversee organizational CMAs and to ensure those agreements comply with the computer matching provisions of the Privacy Act	Low	Moderate	High
Publish Agreements on Website				
DI-2 (1)	Maryland is a state agency and is not required to publish CMAs on the public website.	Low	Moderate	High

Data Minimization and Retention

Data minimization and retention controls assist organizations to collect, use, and retain only relevant PII necessary for the original purpose for which it was collected. The following table outlines the minimum DoIT security control requirements which all Maryland information systems must adhere to in order to operate in a production environment.

Security Control ID	Minimization of Personally Identifiable Information	Security Baselines		
DM-1	The Maryland Agency must: a. Identify the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection b. Limit the collection and retention of PII to the minimum elements identified, for the purposes described in the notice, and for which the individual has provided consent c. Conduct an initial evaluation of PII holdings, and periodically review the holdings, within every **365 days**, to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose The policy must be reviewed and updated at **least every 3 years** and the procedures reviewed and updated **at least annually**.	Low	Moderate	High
Minimization of PII/Locate/Remove/Redact/Anonymize PII				
DM-1 (1)	The Maryland Agency must, where feasible and within the limits of technology, locate and remove/redact specified PII or use anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure.	Low	Moderate	High

Data Retention and Disposal				
DM-2	The Maryland Agency must: a. Retain each collection of PII for the minimum allowable time period necessary to fulfill the purpose(s) identified in the notice or as required by law h. Dispose of, destroy, erase, and/or anonymize the PII, regardless of the method of storage, in accordance with a National Archives and Records Administration (NARA)-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access i. Use legally compliant techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records).	Low	Moderate	High
Data Retention and Disposal/System Configuration				
DM-2 (1)	The Maryland Agency must, where feasible and within the limits of technology, locate and remove/redact specified PII or use anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure.	Low	Moderate	High
Minimization of PII Used in Testing, Training, and Research				
DM-3	The Maryland Agency must: a. Develop policies and procedures that minimize the use of PII for testing, training, and research b. Implement controls to protect PII used for testing, training, and research	Low	Moderate	High
Minimization of PII Used in Testing, Training, and Research/Risk Minimization Techniques				
DM-3 (1)	The Maryland Agency must, where feasible, use techniques to minimize the risk to privacy of using PII for research, testing, or training.	Low	Moderate	High

Individual Participation and Redress

This control addresses the establishment of policy and procedures for the effective implementation of the controls and control enhancements in the IP family. The following table outlines the minimum DoIT security control requirements which all Maryland information systems must adhere to in order to operate in a production environment.

Security Control ID	Consent	Security Baselines		
IP-1	The Maryland Agency must: a. Provide means, where feasible and appropriate, for individuals to authorize the collection, use, maintenance, and sharing of PII before its collection b. Provide appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, or retention of PII c. Obtain consent, where feasible and appropriate, from individuals before any new uses or disclosures of previously collected PII d. Ensure individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII The policy must be reviewed and updated **at least every 3 years** and the procedures reviewed and updated **at least annually**.	Low	Moderate	High
Mechanism Supporting Itemized or Tiered Consent				
IP-1 (1)	The Maryland Agency must implement mechanisms to support itemized or tiered consent for specific uses of data.	Low	Moderate	High

Individual Access				
IP-2	The Maryland Agency must: a. Provide individuals the ability to have access to their PII maintained in its system(s) of records b. Publish policies and/or regulations governing how individuals may request access to records maintained in the system of records c. Publish access procedures d. Adhere to Privacy Act requirements and state policies and guidance for the proper processing of Privacy Act request	Low	Moderate	High
Redress				
IP-3	The Maryland Agency must: a. Provide information to individuals concerning how to contact the relevant organization to have inaccurate PII maintained by that organization corrected or amended, as appropriate b. Establish a process for disseminating corrections or amendments of the PII, if the inaccurate PII was maintained solely by the organization, to other authorized users of the PII, such as external information sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended	Low	Moderate	High
Complaint Management				
IP-4	The Maryland Agency must implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.	Low	Moderate	High
Complaint Management/Response Times				
IP-4 (1)	The Maryland Agency must respond to complaints, concerns, and questions from individuals within a **72-hour** time period.	Low	Moderate	High

Security

This family supplements the security controls which ensure that technical, physical, and administrative safeguards are in place to protect personally identifiable information (PII) collected or maintained by DoIT.

Security Control ID	Inventory of Personally Identifiable Information	Security Baselines		
SE-1	The Maryland Agency must: Establish, maintain, and update within every **365** days, an inventory of all programs and systems used for collecting, creating, using, disclosing, maintaining, or sharing PII Provide each update of the PII inventory to the organization's designated privacy official or information security official to support the establishment of information security requirements for all new or modified information systems containing PII The policy must be reviewed and updated at **least every 3 years** and the procedures reviewed and updated **at least annually**.	Low	Moderate	High
Privacy Incident Response				
SE-2	The Maryland Agency must: a. Develop and implement a Privacy Incident Response Plan b. Provide an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan c. Where applicable, follow current Maryland Law requirements for providing notice to affected parties and reporting incidents to the required organizations, including the Maryland Department of Information Technology and the Maryland Attorney General (AG), as defined in MD State Govt Code § 10-1305 (2017)	Low	Moderate	High

Transparency

This family ensures that organizations provide public notice of their information practices and the privacy impact of their programs and activities.

Security Control ID	Privacy Notice	Security Baselines		
TR-1	The Maryland Agency must: a. Provide effective notice to the public and to individuals regarding: 1. Its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII 2. Authority for collecting PII 3. The choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices 4. The ability to access and have PII amended or corrected if necessary b. Describe: 1. The PII the organization collects and the purpose(s) for which it collects that information 2. How the organization uses PII internally 3. Whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing 4. Whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent 5. How individuals may obtain access to PII 6. How the PII will be protected c. Revise its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before, or as soon as practicable after the change. The policy must be reviewed and updated **at least every 3 years** and the procedures reviewed and updated **at least annually**.	Low	Moderate	High

Real Time or Layered Notice				
TR-1 (1)	The Maryland Agency must provide real-time and/or layered notice to individuals at the time when any PII is collected.	Low	Moderate	High
System of Records notice and Privacy Act Statements				
TR-2	**Non-federal systems are not required to implement this control.** State-based systems must adhere to state laws that may require publication of a notice like the federal System of Records Notices (SORN) and Privacy Act Statement.	Low	Moderate	High
Public Website Publication				
TR-2 (1)	**Non-federal systems are not required to implement this control.** State-based systems must adhere to state laws that may require publication of a notice like the federal SORN and Privacy Act Statement.	Low	Moderate	High
Dissemination of Privacy Program Information				
TR-3	The Maryland Agency must: a. Ensure the public has access to information about its privacy activities and is able to communicate with its designated privacy official. b. Ensure its privacy practices are publicly available through organizational websites or otherwise.	Low	Moderate	High

Use Limitation

This family ensures that organizations only use personally identifiable information (PII) either as specified in their public notices, in a manner compatible with those specified purposes, or as otherwise permitted by law. Implementation of the controls in this family will ensure that the scope of PII use is limited accordingly.

Security Control ID	Internal Use	Security Baselines		
UL-1	The Maryland Agency must use PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices. The policy must be reviewed and updated **at least every 3 years** and the procedures reviewed and updated **at least annually**.	Low	Moderate	High
Information Sharing with Third Parties				
UL-2	The Maryland Agency must: a. Share PII externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes j. When sharing PII, enter into appropriate agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used k. Monitor, audit, and train its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII l. Evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.	Low	Moderate	High

Virtualization Technologies

Agencies must implement careful planning prior to the installation, configuration and deployment of virtualization solutions to ensure that the virtual environment is as secure as a non-virtualized environment and in compliance with all relevant state and/or agency policies. Security should be considered from the initial planning stage at the beginning of the systems development life cycle to maximize security and minimize costs. The security recommendations described in Sections 4 and 5 of NIST SP 800-125 *Guide to Security for Full Virtualization Technologies* must be adopted as the state standard for securing virtualization solutions.

Cloud Computing Technologies

Cloud computing has been defined by NIST as a model for enabling convenient, on- demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction. If an agency plans on using a cloud-based solution for processing, transmitting or storing confidential information, security controls must be implemented to ensure that the compliance and auditing requirements are met as stated in this policy in addition to any federal regulations that may apply.

NIST SP 800-144 *Guidelines on Security and Privacy in Public Cloud Computing (https://csrc.nist.gov/publications/detail/sp/800-144/final)* provides an overview of the security and privacy challenges for public cloud computing and present recommendations that agencies should consider when outsourcing data, applications and infrastructure to a public cloud environment. Maryland agencies must adopt the security recommendations and guidelines described in SP 800-144. The key guidelines recommended to agencies include:

Preliminary Activities;

- Identify security, privacy, and other organizational requirements for cloud services to meet, as a criterion for selecting a cloud provider.
- Analyze the security and controls of a cloud provider's environment and assess the level of risk involved with respect to the control objectives of the organization. A review of the provider's SOC 2 report is helpful.
- Evaluate the cloud provider's ability and commitment to deliver cloud services over the target timeframe and meet the security and privacy levels stipulated.

Initiating and Coincident Activities;

- Ensure that all contractual requirements are explicitly recorded in the service agreement, including privacy and security provisions, and that they are endorsed by the cloud provider.

- Involve a legal advisor in the review of any service agreement and in any negotiations about the terms of service.
- Continually assess the performance of the cloud provider and the quality of the services provisioned to ensure all contract obligations are being met and to manage and mitigate risk.

Concluding Activities;

- Alert the cloud provider about any contractual requirements that must be observed upon termination.
- Revoke all physical and electronic access rights assigned to the cloud provider and recover physical tokens and badges in a timely manner.
- Ensure that organizational resources made available to or held by the cloud provider under the terms of service agreement are returned or recovered in a usable form, and that information has been properly expunged.

Mobile Devices

Tablets, and other mobile computing and communication devices have become very popular because of their convenience and portability. However, the use of such devices is accompanied by risks that must be recognized and addressed to protect both the physical devices and the information they contain. Laptops are specifically excluded from the scope of this policy because the security controls available for laptops today are quite different than those available for mobile devices.

The most effective way to secure confidential data is not to store it on mobile devices. As a matter of policy and best practice, data should always be secured where it resides.

State business requirements may, on occasion, justify storing confidential data on mobile computing devices. In these cases, Agencies are required to assure that steps have been taken to keep the data secure. It is the responsibility of the agencies to recognize these risks and take the necessary steps to protect and secure their mobile computing devices. Consideration of a mobile device management solution may be necessary to implement recommended controls.

Steps may include, but are not limited to:

- Maintaining a list of supported mobile devices.
- Protecting data transmission that occurs between the mobile device and the agency assets.
- Protecting data storage on mobile devices including removable media.
- Implementing procedures that should be followed if a mobile device is lost or is at risk of having its data recovered by an untrusted party (proper

authority notification and device wipe options).

- Requiring that all vendor recommended patches, hot-fixes or service packs must be installed prior to deployment and processes must be in place to keep system hardware, operating system and applications current based on vendor support recommendations (including patches, hot-fixes, and service packs);
- Applying proper asset management procedures to all mobile devices;
- Whenever possible, centrally controlling and managing all mobile device application distribution and installation;
- Whenever possible, centrally controlling and managing all mobile device operating system and application security patch installation;
- Disabling Mobile device options and applications that are not in use;
- Whenever possible, configuring Bluetooth settings to notify users of incoming connection requests and to receive confirmation before proceeding;
- Enabling password or PIN protection on all mobile devices;
- Enabling timeout/locking features and device erase functions (including removable memory) on all mobile devices;
- Whenever possible, all mobile devices should have anti-virus and/or firewall protection installed;
- No confidential information must be stored on mobile devices unless it is encrypted, and permission is granted from an authorized official;
- Confidential information should be sanitized from the mobile device before it is returned, exchanged or disposed of; and
- Whenever possible, mobile devices must be scanned for viruses/malware before they can connect to state systems;

The physical security of state issued mobile devices is the responsibility of the employee to whom the device has been assigned. Devices must be kept in the employee's physical presence whenever possible. Whenever a device is being stored, it must be stored in a secure place, preferably out-of-sight. If a mobile device is lost or stolen, the employee is responsible for promptly reporting the incident to the proper authorities and all business applications must be wiped.

Data Loss Prevention Guidance

If currently implemented security controls have failed to reduce agency information security risk to an acceptable level, a data loss prevention solution should be considered.

Data loss prevention (DLP) refers to a comprehensive approach covering people, processes, and systems that identify, monitor, and protect data in use, data in motion, and data at rest, through deep content inspection and with a centralized management framework. DLP solutions go beyond securing the network to securing systems within the network, and to securing the data itself. DLP controls are based on policy, and include classifying sensitive data, discovering that data across an enterprise, enforcing controls, and reporting and auditing to ensure policy compliance. A comprehensive DLP solution should include the following controls.

- Use network monitoring tools to analyze outbound traffic looking for anomalies which may include; large file transfers, long-time persistent connections, connections at regular repeated intervals, unusual protocols and ports in use, and possibly the presence of certain keywords in the data traversing the network perimeter;
- Deploy an automated tool on network perimeters that monitors for certain sensitive information (e.g., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel;
- The ability to scan systems using automated tools to determine whether confidential data is present in clear text;
- Use outbound proxies to be able to monitor and control all information leaving an organization;
- Use secure, authenticated, and encrypted mechanisms to move data between untrusted networks;
- If there is no business need for supporting such devices, organizations should configure systems so that they will not write data to USB tokens or USB hard drives. If such devices are required, enterprise software should be used that can configure systems to allow only specific USB devices (based on serial number or other unique property) to be accessed, and that can automatically encrypt all data placed on such devices. An inventory of all authorized devices must be maintained;
- Monitor all traffic leaving the organization and detect any unauthorized use of encryption. Attackers often use an encrypted channel to bypass network security devices. Therefore, it is essential that organizations be able to detect rogue connections, terminate the connection, and

remediate the infected system.
- DLP solutions should be tested periodically with results documented. Results of the tests can help identify if a business or technical process is leaving behind or otherwise leaking confidential information.

Enforcement

Data leakage incidents such as disclosure of non-public information or making inappropriate public statements about or for the State/agency, or using state resources for personal uses, and harassing or inappropriate behavior toward another employee can be grounds for reprimand or dismissal. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Deliberate, unauthorized disclosure of non-public information may result in civil and/or criminal penalties. Failure to comply with any provisions of the DoIT IT Security Manual may result in administrative or adverse action. Any individual with access to state systems or networks who introduces or is associated with perceived threats to system integrity, confidentiality, or availability may be subject to suspension of system access as necessary to contain the perceived threat. An offense that is in violation of local, state, or Federal laws may result in suspension of system access and must be reported to the appropriate law enforcement authorities.

DoIT IT security policies must be enforced through the following:
- Oversight
- Inspection
- Audit

The relevant Contracting Officer (CO) has contract oversight of security responsibilities and must ensure that contractor-related security requirements are followed throughout the contract life-cycle.

Risk Assessment Policy

The Maryland Department of Information Technology (DoIT) requires Maryland Information Systems (MIS) and vendors that store, process, or transmit State of Maryland (State) data to adhere to certain security related standards. Adherence to the standards outlined in this document provides assurance that, at a minimum, the MIS/vendor organization has implemented the appropriate security controls associated with the following five (5) Trusted Service Principles:

I. **Security:** Systems are protected both logically and physically against unauthorized access.
II. **Availability:** Systems are available for operational use, for vendor systems this would be as committed through the vendor organization's agreed Service-Level Agreement (SLA).

III. **Processing Integrity:** Processing is complete, accurate, timely, and authorized. It is required that data integrity is maintained throughout its lifecycle and is protected from unauthorized modifications.
IV. **Confidentiality:** Sensitive information that is stored, processed, and/or transmitted through any system is protected from unauthorized disclosure and is only available to authorized users.
V. **Privacy:** The responsible organization collects, manages, and reports on state-owned sensitive data in a manner that is consistent with the privacy principles defined by the American Institute of Certified Public Accountants (AICPA), Maryland privacy laws, and federal privacy laws.

Purpose

The State is committed to ensuring that all systems and vendor organizations that store, process, or transmit state-owned data on an external information system meet, at minimum, basic compliance requirements. Dependent on the classification level of the system and associated data, the compliance requirements will necessarily vary. The compliance requirements, based on system and data classification, are provided in this document. This document also outlines conditions, frequencies, and procedures for validating compliance for vendor organizations both initially and on a continuing basis.

Conditions

MIS/vendor organizations must provide evidence that they are compliant with the classification process provided in the *System Security Categorization section of this IT Security Manual.* Additionally, vendors are required to meet the minimum controls identified within the *Vendor Required Security Controls* section below, if:

- The vendor organization stores, processes, or transmits state-owned data on their hosted information system;
- The vendor organization's information system interconnects with a state information system;
- The vendor organization's information system contains references, pointers and metadata associated to actual state-owned data; or
- The vendor organization is developing an application that stores, processes and/or transmits sensitive state data within a state-hosted environment (Partial requirements) – processing integrity and privacy principles for administrative controls.

Vendor Required Security Controls

Vendor-hosted information systems must, at a minimum, implement the following controls for "**Low**" categorized systems. Selection and implementation of controls must be in accordance with DoIT guidelines and policy:

Access control – The organization must implement technical access restrictions to ensure that only authorized individuals may access the vendor-hosted environment.

Identification and Authentication – The organization must ensure that authorized individuals will be uniquely identified while operating within the vendor-hosted environment. Identifiers must be traceable and non-reputable to preserve accountability. The organization will restrict the use of shared accounts unless authorized by the State.

Auditing and Accountability – The organization must implement a logging solution to capture all activity that occurs within the environment. At minimum, the organization must log the following events:

- Login/Logoff
- Code Commits
- Configuration Changes
- File upload/download transactions

Additionally, the content of each audit record must contain the following:

- Date/Time of Event
- Type of Event
- Source of Event
- Outcome of Event

The organization must restrict access to audit log information with the intent of evidence preservation. The organization must provide a list of individuals with access to audit logs.

In addition to the “Low” control requirements, vendor systems that have been classified as a “**Moderate**” are required to implement the following. Selection and implementation of controls must be in accordance with DoIT guidelines and policy:

Encryption – The organization must ensure that encryption is enabled for both data-in transit and at-rest where applicable. At minimum, the organization must use TLS 1.2 and/or AES-256 based cipher methods.

Data Restrictions – The organization is restricted from transmitting and/or using state production-level data within the development environment. The organization must notify the state of data restriction violations within (1) hour of discovery.

Secure Development Practices – The organization must ensure that secure development practices are exhibited within the vendor-hosted environment. The organization is responsible for ensuring that staff is adequately trained in the latest security practices.

Platform Hardening – The organization must only develop systems/applications using operating system and software versions that are consistent with the State's approved baselines.

Vulnerability Scans – The organization must perform vulnerability scans (Weekly) to ensure that flaws are not introduced to the environment. The organization must make the vulnerability scan results available to the state upon request.

Source Code Review – The organization must perform source code reviews using a Static Code Analysis (SCA) tool prior to code commits. The organization must correct any flaws identified during the review process prior to promoting code to the production environment.

Procedures

A vendor organization that stores, processes or transmits State of Maryland data must provide a Risk Assessment Report (RAR) to the DoIT Security Team, which must be approved before any sensitive or production level data is allowed to be stored, processed, or transmitted by a vendor system, or otherwise handled by a vendor. The RAR must meet the following criteria:

- Contains system and associated data classification details and justification for why a classification level was chosen
- Contains complete security control implementation details
- Identifies any non-compliant controls and their remediation plans/timelines
- Organizational Points of Contact

A SOC-2 report is deemed an acceptable form of risk assessment and will count as a compliant RAR for the purposes of this document. Vendor organizations need not submit a separate RAR if they are able to produce a SOC-2 report showing SOC-2 compliance. If a vendor organization elects to use a SOC-2 report, it must be certified and audited by an authorized accounting firm (evidence of attestation).

The DoIT Security Team will review/validate the provided RAR/SOC-2 report and any associated artifacts within ten (10) business days upon receiving.

Following the initial validation, the vendor organization's compliance will be reviewed on an annual basis.

However, if the vendor's RAR/SOC-2 report identifies any non-compliant controls, DoIT will request updates periodic updates on their remediation status at the

following frequencies, based on the associated risk/criticality:

- Critical/High Risk – Risk Memorandum required, Monthly Check-In (See *Risk Acceptance Policy* for Risk Memorandum procedures)
- Medium/Low Risk – No waiver required, bi-annual check-in

A partial RAR/SOC-2 report may be requested from the vendor organization in the event it is contracted to perform work on state systems. The specific request criteria for partial RAR/SOC-2 reports will be made by the DoIT Security Team on a case-by-case basis and communicated from the Awarding Agency to the vendor organization prior to the contract award. All procedures outlined in this document are applicable to any partial RAR/SOC-2 scenarios.

All communication and artifact submissions regarding RAR/SOC-2 activities will be directed to the Awarding Agency and the DoIT Security Team, this will be defined for the vendor organization prior to contract award. Any information received from the vendor organization will remain confidential and will not be shared outside the Awarding Agency and DoIT Security Team.

Risk Acceptance Policy

The Maryland Department of Information Technology (DoIT) provides IT services to state agencies in support of day-to-day operations, program initiatives and overall missions. Enterprise-level IT infrastructure requires rigorous administration, maintenance and upkeep to stay relevant and defend against evolving cyber threats. As such, agencies that receive IT services from DoIT (such as network or hosted infrastructure) inherit the operational, management, and technical benefits associated with DoIT's security program, thereby alleviating the receiving agency's administrative burden.

As a part of DoIT's robust security practice, DoIT regularly performs flaw remediation on IT assets under the Department's purview. This includes:

- Security Control Implementation
- Security patches and hotfixes
- Vendor-provided updates
- Software version upgrades

When flaw remediation activities are performed, affected agencies are informed and collaborated with, when applicable. It is noted that this process only applies to software that is currently supported by the originating vendor.

Risk Acceptance Memorandum Process

DoIT acknowledges that risk acceptance conditions may differ based on the circumstances presented by the agency seeking a risk waiver. DoIT implements a Risk Acceptance Waiver Process for the following risk-based conditions:

Non-compliance of Security Controls

Agencies are required to document and track all control weaknesses as Plan of Action and Milestones (POA&M) for all systems that cannot meet the security control requirements designated within this Manual. For additional regarding POA&M requirements, see control *CA-5: Plan of Action and Milestones*.

However, if the agency is unable to meet the control requirements due to organizational constraints (ex. lack of funding, resources, etc.) for a period that exceeds (1) year, DoIT will grant a Risk Acceptance Memorandum for the agency under the following conditions:

- The agency consults with DoIT and provides sufficient justification, commensurate with the nature of the risk, for not meeting the security control requirements defined within this Manual;
- The agency consults with DoIT and develops a roadmap to implement the required security controls. The roadmap must be approved and acknowledged by DoIT;
- The agency develops a detailed project plan that identifies dates and milestones for all activities leading up to the remediation of the non-compliant security control.

When all conditions are met, DoIT will issue a *Risk Acceptance Memorandum* (RAM) to the agency for a defined period in which DoIT will accept the risk(s) associated with the non-compliance. Additionally, the agency will provide progress updates to DoIT every (6) months until the issue has been fully remediated. Vendors receiving RAMs will be required to provide progress updates to the contracting agency on a monthly/bi-annual frequency depending on the severity of non-compliant security control(s).

Unsupported Software

For DoIT supported agencies that have a business need to use unsupported software, DoIT requires completion of DoIT's Risk Acceptance Process. Unsupported software is software for which the software vendor no longer provides security updates or patches. As a part of the process, the supported agency assumes the risk associated with the use of unsupported software. Additionally, the supported agency acknowledges that the use of unsupported software will result in non-compliance with DoIT IT Security Standards mandated by the State and could therefore also cause the supported agency to incur audit findings.

As a part of the Risk Acceptance Process, any supported agency using unsupported software will be required to complete a RAM, which must be signed by the supported agency Authorizing Official (AO). The RAM will be active and the supported agency will assume the risk of using unsupported software until decommission.

On a bi-annual cycle, DoIT will identify and validate the use of unsupported software across the hosted environment. Upon validation, DoIT will perform one of the following actions:

1. Initial/new detections of unsupported software will require that the affected supported agency complete a new RAM;

2. Continual detections of unsupported software will require the affected supported agency to re-sign the existing RAM;

3. Close existing RAM agreements where unsupported software has been decommissioned.

In situations where unsupported software is necessary due to legacy requirements, DoIT strongly recommends that the supported agency consider corrective actions wherever feasible, including replacement/updates of legacy systems. DoIT is committed to improving the State's cybersecurity posture and will offer guidance for developing long-term remediation strategies upon request.

Definitions

Supported Agency: An agency that receives IT services from DoIT (such as network or hosted infrastructure), and thereby inherits operational, management, and technical benefits associated with DoIT's security program.

Authorizing Official (AO): A supported agency official with the authority to formally assume responsibility for operating an information system and accept any risk to State/agency operations (including mission, functions, image, or reputation), agency assets, or individuals.

Procurement Policy

Development-Hosted Contract Requirements

For service organizations that develop systems and applications within their own hosted environment, the Maryland Agency must require the organization have the following operational, management and technical in place:

Access control – The organization must implement technical access restrictions to ensure that only authorized individuals may access the development environment.

Identification and Authentication – The organization must ensure that authorized individuals will be uniquely identified while operating within the development environment. Identifiers must be traceable and non-reputable to preserve accountability. The organization will restrict the use of shared accounts unless authorized by the State.

Auditing and Accountability – The organization must implement a logging solution to capture all activity that occurs within the environment. At minimum, the organization must log the following events:

- Login/Logoff
- Code Commits
- Configuration Changes
- File upload/download transactions

Additionally, the content of each audit record must contain the following:

- Date/Time of Event
- Type of Event
- Source of Event
- Outcome of Event

The organization must restrict access to audit log information with the intent of evidence preservation. The organization must provide a list of individuals with access to audit logs.

Encryption – The organization must ensure that encryption is enabled for both data-in transit and at-rest where applicable. At minimum, the organization must use TLS 1.2 and/or AES-256 based cipher methods.

Data Restrictions – The organization is restricted from transmitting and/or using state production-level data within the development environment. The organization must notify the state of data restriction violations within (1) hour of discovery.

Secure Development Practices – The organization must ensure that secure development practices are exhibited within the hosted environment. The organization is responsible for ensuring that staff is adequately trained in the latest security practices.

Platform Hardening – The organization must only develop systems/applications using operating system and software versions that are consistent with the State's approved baselines.

Vulnerability Scans – The organization must perform vulnerability scans (Weekly) to ensure that flaws are not introduced to the environment. The organization must make the vulnerability scan results available to the state upon request.

Source Code Review – The organization must perform source code reviews using a Static Code Analysis (SCA) tool prior to code commits. The organization must correct any

flaws identified during the review process prior to promoting code to the production environment.

Right to Audit – The State reserves the right to audit the organization at will. Audits must be performed either by the State or a trusted third-party. The organization agrees and must provide evidence/artifacts as requested by the auditor.

Production-Hosted Contract Requirements

For service organizations that host production systems/applications containing sensitive data (PII, PHI, FTI) within their environment, the State requires the organization meet at least (1) of the following requirements:

1. Cloud Environment – The offering must be FedRAMP Authorized at a Moderate (IaaS, PaaS, SaaS)
2. Non-Cloud Environment – The offering must be SOC II Type II compliant

For organizations that do not meet either requirement, the State may elect to perform a security evaluation of the hosted environment. The evaluation will be based on the implementation of security controls consistent with NIST Special Publication 800-53 R4: *Security and Privacy Controls for Federal Information Systems and Organizations*. At minimum, the State will evaluate the following security control families:

- Access Control
- Auditing and Accountability
- Identification and Authentication
- Systems and Communication Protection
- Configuration Management
- System and Information Integrity Protection
- Incident Response
- Contingency Planning

The State may accept a positive, security evaluation in lieu of the requirements identified above.

Appendix A: Security Authorization Checklist

The following provides a list of security artifacts required for each Maryland Information System in order to make a determination by the Maryland Agency's Authorizing Official (AO) to grant an Authority To Operate (ATO):

Initial Authorization Package	
☐	**MIS Security Plan (SSP)**
☐	**Organizational IT Policies**
☐	**Electronic Authentication (E-Authentication) Assessment**
☐	**Privacy Threshold/ Impact Assessment (PTA/PIA)**
☐	**Rules of Behavior (ROB)**
☐	**Contingency Plan (CP)**
☐	**Continuous Monitoring Plan**
☐	**System Inventory (Hardware/Software/Firmware)**
☐	**Incident Response Plan (IRP)**
Assessment Artifacts	
☐	**Security Assessment Plan (SAP)**
☐	**Security Requirements Traceability Matrix (SRTM)**
☐	**Security Assessment Report (SAR)/ Risk Assessment Report (RAR)**
Technical/Supporting Artifacts	
☐	**System Detailed Design Document**
☐	**High-Level Architecture (Designs/Diagrams)**
☐	**Configuration Management Plan**
☐	**Configuration Baselines and Guides**
☐	**List of System Accounts and Privileges**

Appendix B: IT Incident Reporting Form

Incident Reporting Instructions

This form is to be completed as soon as possible following the detection or reporting of an Information Technology (IT) security incident. All items completed should be based on information that is currently available. This form may be updated and modified if necessary.

Incident Reporting Form

1. Government Contact Information for this Incident	
Name:	
Title:	
Program Office:	
Work Phone:	
Email address:	
2. Contractor Contact Information for this Incident	
Name:	
Title:	
Program Office:	
Work Phone:	
Email Address:	
3. Incident Description.	
Provide a brief description:	
4. Impact / Potential Impact Check all of the following that apply to this incident.	
□ Loss / Compromise of Data □ Damage to Systems □ System Downtime □ Financial Loss □ Other Organizations' Systems Affected □ Damage to the Integrity or Delivery of Critical Goods, Services or Information □ Violation of legislation / regulation □ Unknown at this time	

Provide a brief description:

5. Determine the Sensitivity of Data	
Category	**Example**
Public	This information has been specifically approved for public release by Public Relations department or Marketing department managers. Unauthorized disclosure of this information will not cause problems for the Department of Maryland, its customers, or its business partners. Examples are marketing brochures and material posted to Department of Maryland web pages. Disclosure of agency information to the public requires the existence of this label, the specific permission of the information Owner, or long-standing practice of publicly distributing this information.
Internal Use Only	This information is intended for use within DoIT and Maryland Information Systems (MIS) or between agencies, and in some cases within affiliated organizations, such as business partners. Unauthorized disclosure of this information to outsiders may be against laws and regulations, or may cause problems for the Department of Maryland, its customers, or its business partners. This type of information is already widely distributed within the Department of Maryland, or it could be so distributed within the organization without advance permission from the information owner. Examples are an agency telephone book and most internal electronic mail messages.
Restricted/Confidential (Privacy Violation)	This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access. Unauthorized disclosure of this information to people without a business need for access may be against laws and regulations or may cause significant problems for the Department of Maryland, its customers, or its business partners. Decisions about the provision of access to this information must be cleared through the information owner. Examples are customer transaction account information and worker performance evaluation records. Other examples include citizen data and legal information protected by attorney-client privilege.
Information Involved. Check all of the following that apply to this incident.	

Unknown/Other	Describe in the space provided
□ Public □ Internal Use Only	□ Restricted / Confidential (Privacy violation) □ Unknown / Other – please describe:
Provide a brief description of data that was compromised:	
6. Who Else Has Been Notified?	
Provide Person and Title:	

Appendix C: Acronyms and Abbreviations

Acronym	Definition
AC	Access Control
AO	Authorizing Official
AP	Authority and Purpose
AR	Accountability, Audit, and Risk Management
AT	Awareness and Training
ATO	Authority to Operate
AU	Audit and Accountability
C3	CISCO Command Center
CERT	Computer Emergency Readiness Team
CFO	Chief Financial Officer
CIPM	Critical Infrastructure Protection Manager
CISO	Chief Information Officer
IRT	Incident Response Team
CITR	Commerce Interim Technical Requirement
CM	Configuration Management

CNSS	Committee on National Security Systems
CO	Contracting Officer
COOP	Continuity of Operations
CCO	Contracting Officer's Technical Representative
CP	Contingency Plan or Planning
CPIC	Capital Planning and Investment Control
CTO	Chief Technology Officer
DATO	Deny Authorization to Operate
DHCP	Dynamic Host Configuration Protocol
DI	Data Quality and Integrity
DM	Data Minimization and Retention
DNS	Domain Name System
DOO	Department Organization Order
EA	Enterprise Architecture
EPMS	Enterprise Program Management System
EPO	Emergency Power Off
FFMIA	Federal Financial Management Improvement Act

FIPS	Federal Information Processing Standards
FISCAM	Federal Information Systems Controls Audit Manual
FISMA	Federal Information Security Management Act of 2002
FISMA	Federal Information Security Modernization Act of 2014
FTP	File Transfer Protocol
FMFIA	Federal Managers' Financial Integrity Act
FQDN	Fully Qualified Domain Name
GAO	Government Accountability Office
GISRA	Government Information Security Reform Act
GPEA	Government Paperwork Elimination Act
GPRA	Government Performance and Results Act
GSA	General Services Administration
GUI	Graphical User Interface
HSPD	Homeland Security Presidential Directive
IA	Identification and Authentication
IDS	Intrusion Detection Systems
IEO	Office of Infrastructure Engineering and Operations

IMAP	Internet Message Access Protocol
INFOSEC	Information Systems Security
IP	Individual Participation and Redress
IR	Incident Response
ISSO	Information System Security Officer
IT	Information Technology
LAN	Local Area Network
MA	Maintenance
MIS	Maryland Information System
MP	Media Protection
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NNTP	Network News Transfer Protocol
OAED	Office of Application Engineering and Development
OCISO	Office of the Chief Information Officer
OGC	Office of General Counsel
AG	Office of Inspector General

OIMS	Office of Information Management Services
OMB	Office of Management and Budget
OPAO	Office of Program Administration Organization
OPG	Office of Organizational Policy and Governance
OPI	Office of Primary Interest
OS	Operating System
PE	Physical and Environmental Protection
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PL	Planning
PM	Project Manager
POA&M	Plan of Action and Milestones
POC	Point of Contact
POP	Post Office Protocol
PRA	Preliminary Risk Assessment

PS	Personnel Security
RA	Risk Assessment
RAR	Risk Assessment Report
RBAC	Role Based Access Control
RoB	Rules of Behavior
RPC	Remote Procedure Call
SA	System and Services Acquisition
SAP	Security Authorization Package
SAR	Security Assessment Report
SC	System and Communication Protection
SDLC	System Development Life Cycle
SE	Security
SI	System and Information Integrity
SO	System Owner
SOP	Standard Operating Procedure
SORN	Systems of Records Notices
SP	Special Publication

SSH	Secure Shell
SSP	System Security Plan
ST&A	Security Test and Assessment
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
TL	Technical Lead
TR	Transparency
UL	Use Limitation
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team
USGCB	US Government Configuration Baseline
DoIT	Department of Information Technology
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network

Appendix D: Glossary

Term	Definition
Acceptable Level of Risk	A judicious, carefully considered, and fully documented assessment by the appropriate Designated Approving Authority (AA) that an information subsystem meets the minimum requirements of applicable security directives. The assessment should take into account and carefully document the sensitivity and criticality of information, threats, vulnerabilities and countermeasures and their effectiveness in compensating for vulnerabilities, and operational requirements.
Acceptable Risk	A concern that is deemed acceptable to responsible management, due to the cost and magnitude of implementing countermeasures to mitigate the risk.
Accountability	Accountability is (1) The quality or state that enables violations or attempted violations of IT Security to be traced to individuals who may then be held responsible. (2) The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, after-action recovery and legal action.
Adequate Security	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.
Application	The use of information resources (information and information technology) to satisfy a specific set of users requirements (See Major Application).
Assessment	See Security Control Assessment

Assurance	Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. Adequately met includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software, and (3) sufficient resistance to intentional penetration or bypass.
Audit Log	A chronological record of system activities which enables the reconstruction and examination of the sequence of events and activities surrounding or leading to an operation, a procedure or an event in a transaction from its inception to final results. The audit log also serves as the chain of custody for the history of use of a record. This term is synonymous with Audit Records and Audit Trails.
Authentication [FIPS 199]	The process of verifying the identity of a user, process or device, often as a prerequisite to allowing access to resources in an information system.
Publicly Accessible System	Systems such as Web and FTP applications that are exposed to the Internet and therefore, more vulnerable.
Public Information	Information that is a public record under the Maryland Public Information Act.
Remote Access	Any access to DoIT ’s managed network through a non-DoIT managed network, device, or medium.
Sanitization	Refers to the general process of removing data from storage media, such that there is reasonable assurance that the data may not be easily retrieved and reconstructed.
Sensitive	Information that, if divulged, could compromise or endanger the citizens or assets of the State.

Social Media	Online technologies and practices that people use to share opinions, insights, experiences, and perspectives with each other.
SNMP	Simple Network Management Protocol is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.
SSH	Secure Shell is a network protocol that allows data to be exchanged using a secure channel between two computers.
SSID	Service Set Identifier is a name used to identify the particular 802.11 wireless LAN to which a client wants to attach.
Untrusted Entity	An entity that can or may be potentially harmful to a system.
Wi-Fi Certified	Wi-Fi CERTIFIED is a program for testing products to the 802.11 industry standards for interoperability, security, easy installation, and reliability
Publicly Accessible System	Systems such as Web and FTP applications that are exposed to the Internet and therefore, more vulnerable.

Appendix E: Wireless Security

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to any state agency network. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by the Agency CIO (or similar delegated Agency authority) are approved for connectivity to agency networks. Agencies must;

Register Access Points

All wireless Access Points / Base Stations connected to the network must be registered and approved by DoIT. All approved Access Points / Base Stations are subject to periodic penetration tests and audits.

Approved Technology

All wireless LAN hardware implementations must utilize Wi-Fi certified devices that are configured to use the latest security features available.

Physical Location

Security mechanisms should be put in place to prevent the theft, alteration, or misuse of Access Points / Base Stations. All devices must be locked and secured in an appropriate manner.

Configuration

The default SSID and administrative username / password must be changed on all Access Points / Base Stations. Device management must utilize secure protocols such as HTTPS and SSH. If SNMP is used in the management environment, change all default SNMP community strings, otherwise disable it. Access Points / Base Stations should be placed strategically and configured so that the SSID broadcast range does not exceed the physical perimeter of the building. If configurable, adjust the SSID beacon transmission rate to the highest value. Console access must be password protected.

Authentication and Transmission

All wireless access points that connect clients to the internal network (LAN) must require users to provide unique authentication over secure channels and all data transmitted must be encrypted with an approved encryption technology.

Internet-only Deployments

Access Points / Base Stations deployed to provide Internet-only service must be separated from the internal network by denying all internal services. Access Point / Base Station management must be limited to internal or console users and not available to wireless clients.

Failure to Comply

Any exception to the policy must be approved by the information security team in advance. Violations of this wireless security policy may result in disciplinary / corrective action up to and including termination of employment. Users may additionally be subject to loss of network privileges and, in cases where appropriate, civil and/or criminal prosecution. DoIT and Maryland Information Systems (MIS) Chief Information Security Officer (CISO) is responsible for enforcement of this policy. All users of the network within DoIT and Maryland Information Systems (MIS) are required to report any violations of this policy to the CISO.

Appendix F: Sample Media Sanitization Form

Instruction for Media Sanitization Form

This form is to be completed during the disposal of any media or system components, especially that which contains PII or sensitive information. All items completed should be based on information that is currently available. This form must be finalized by the individual validating the information and process of the disposal method being used.

Media Sanitization Form				
Organization Name:				
Description of Item:				
Item Disposition:				
Special Handling due to PII? Yes/No				
Sanitization/ Destruction Time Stamp	**Date:**		**Time:**	
Individual Conducting Media Sanitization				
Name:				
Email:				
Program Office				
Work Phone:				
Validation				
Name:				
Email:				
Program Office				
Work Phone:				
Sanitization Method Used				
Describe/Identify the method used for sanitizing the item				

Appendix G: Sample Incident Handling Checklist and Forensics Guidelines

Action	Done
Detection and Analysis	
Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
Identify which resources have been affected and forecast which resources will be affected	
Report the incident to the appropriate internal personnel and external organizations	
Containment, Eradication, and Recovery	
Acquire, preserve, secure, and document evidence	
Contain the incident	
Eradicate the incident	
Identify and mitigate all vulnerabilities that were exploited	
Remove malicious code, inappropriate materials, and other components	
Recover from the incident	
Return affected systems to an operationally ready state	
Confirm that the affected systems are functioning normally	
If necessary, implement additional monitoring to look for future related activity	
Post-Incident Activity	
Create a follow-up report	
Hold a lessons learned meeting	

Refer to the corresponding tables within NIST SP 800-61 Revision 2 *Computer Security Incident Handling Guide* for specific incident category guidance.

Incident Response and Forensics Guidelines

Preserving forensic data is an essential aspect of any incident response plan. The forensic data acquired during the overall incident response process is critical to containing the current intrusion and improving security to defend against a similar future attack. The following guidelines are provided to assist agencies in the retention of essential forensic data.

Keep detailed notes of all observations, including dates/times, mitigation steps taken/not taken, device logging enabled/disabled, and machine names for suspected compromised equipment. More information is generally better than less information.

When possible, capture live system data (e.g., current network connections and open processes) prior to disconnecting a compromised machine from the network.

Capture a forensic image of the system memory prior to powering down the system.

When powering down a system, physically pull the plug from the wall rather than gracefully shutting down. Forensic data can be destroyed if the operating system (OS) executes a normal shut down process.

After shutting down, capture forensic images of the host hard drives.

Avoid running any antivirus software “after the fact” as the antivirus scan changes critical file dates and impedes discovery and analysis of suspected malicious files and timelines.

Avoid making any changes to the OS or hardware, including updates and patches, as they might overwrite important information relevant to the analysis. Organizations should consult with trained forensic investigators for advice and assistance prior to implementing any recovery or forensic efforts.

When a compromised host is identified, it should be removed from the network for forensic data collection (but not powered off, as noted above). When all available data have been retained from the infected host, agencies should follow established internal procedures for recovering the host.

If an agency does not have an adequate incident response plan or the necessary staff to handle a serious cyber incident, it should consult trained forensic investigators to assist with developing a response plan and implementing recovery efforts.

Useful imaging tools can be used to capture and preserve evidence.

End of Document