Frederick County Public Schools (FCPS) Department of Technology Infrastructure (DTI) Information System Security Manual

FCPS Written Information Security Program (WISP)

Revision History

Version #	Date	Author	Description
1.0	April 2019	Edward Gardner	Initial Document
2.0	September 2019	Edward Gardner	Updates to Reflect MD DoIT Security Manual Version 1.2
3.0	September 2020	Edward Gardner	Annual Review
4.0	November 2021	Edward Gardner	Annual Review

Table of Contents

FCPS Information System Security Manual

1 Overview

1.1. 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 Information Technology (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)
- Payment Card Industry Data Security Standards (PCI DSS)
- IRS Publication 1075 - Tax Information Security Guidelines for Federal, State, and Local Agencies Manual (FISCAM)
- Maryland Executive Order 01.01.2017.22
- Maryland State Government Article Title 10 Subtitle 13
- National Technology Transfer and Advancement Act of 1996
- National Institute of Standards and Technology (NIST) Special Publications
- Office of Legislative Audits (OLA)
- Office of Management and Budget (OMB) Circulars
- OMB Memoranda
- Privacy Act of 1974
- Family Educational Rights and Privacy Act (FERPA)
- Children's Online Privacy Protection Act (COPPA)
- Children's Internet Protection Act (CIPA)
- Individuals with Disabilities Education Act (IDEA)
- Every Student Succeeds Act (ESSA)
- Rehabilitation Act Sections 504 & 508
- Gramm-Leach-Bliley Act (GLBA)
- Maryland Code, State Finance and Procurement § 3A-303 and § 3A-305

The State of Maryland and Frederick County Government routinely assess the implementation of these standards.

The Frederick County Public Schools Board of Education (FCPS BoE) has the authority to set policy, provide guidance, and oversight to meet the security and privacy requirements of DoIT, the Maryland State Chief Information Security Officer (CISO), and all applicable laws and regulations, for all IT systems employed by the Frederick County Local Education Agency (LEA). The FCPS BoE has passed Policy 208 Data Security requiring the Superintendent to establish regulations, which will implement and maintain a Written Information Security Program (WISP).

Regulation 200-32 Data Security defines the WISP as a comprehensive documented record defining the framework necessary to provide for the security of the confidentiality, integrity, and accessibility of FCPS information. The minimum level of technical security controls and data privacy practices necessary to meet the legal & regulatory standards, as sighted above, and mitigate FCPS information risk to within an acceptable level for all student and staff information systems.

This Frederick County Public Schools Information System Security Manual has been developed to meet all mandated requirements and is authorized by law, policy, regulation, and guidance for enforcement within FCPS.

1.2. Purpose

This manual provides guidance, instructions and required formats for a Frederick County Public Schools (FCPS) information system security operations and documentation. The information security framework defined in this manual is designed in direct support of the requirements of FCPS Board of Education (BoE) Policy 208 and Regulation Number 200-32 Data Security, for FCPS to maintain a Written Information Security Program (WISP).

These guidelines and instructions apply to all FCPS entities responsible for administering the Operations and Maintenance of information system boundaries. This document serves as the primary manual for establishing and defining the FCPS mandated IT security practices and requirements for the entire organization.

The IT security policies captured within this manual were developed to align with the federal and state government standards and procedures issued by the Maryland State Department of Information Technology (MD DoIT), 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), the General Services Administration (GSA), Health Insurance Portability and Accountability Act (HIPAA), and others.

Additional security requirements may be added by the FCPS Department of Technology Infrastructure (DTI) to an information security boundary, based on the assessment of risk and security requirements, which may exceed the minimum-security standards expressed in this manual.

1.3. Scope

The WISP, as defined in this manual, applies to any Information System (IS) that electronically generates, receives, stores, processes or transmits FCPS-owned data, whether the system is hosted on the FCPS network or by a third-party provider. The provisions of this manual also apply to all FCPS employees, contractors, and potential information system users (both internal and external). This document has been developed and is owned by the FCPS DTI, the requirements and provisions herein are drafted in compliance with the guidance provided by the MD DoIT and the Maryland State Chief Information Security Officer.

1.4. Overview

Each Information System Owner (ISO) must produce and maintain a formally approved Authorization to Operate (ATO) package for the information security boundary, for which they have management responsibility. The ATO Package shall contain information about cyber security measures taken by the ISO on behalf of FCPS, for the protection of information technology systems and data.

2 Preface

Information and information technology (IT) systems are essential assets of FCPS and vital resources to staff, students, and the public. These assets are critical to the services that FCPS provides on behalf of the public. All information, products, and systems created with FCPS resources are the property of the FCPS BoE. All employees and contractors of FCPS are responsible for protecting such information and resources from unauthorized access, modification, disclosure, and destruction. This manual sets forth a minimum level of security requirements that, when implemented, will provide the basis for protecting the confidentiality, integrity, and availability (CI&A) of FCPS Information Systems (IS) and FCPS-owned data.

The State of Maryland assesses and publicly reports the security of FCPS ISs based on the requirements documented within the MD DoIT State of Maryland Information Technology Security Manual Version 1.2 (June 28, 2019). The MD DoIT manual has adopted NIST information security related standards and guidelines. 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 quality of life.

FCPS Departments should[1] develop procedures to ensure compliance with the standards defined in this manual. If there is no applicable published NIST standard or a published standard is deemed insufficient, the FCPS DTI will adopt industry accepted security guidelines (or develop them) and refer to them within the security manual.

This manual enumerates information system management, operational, and technical controls to a moderate level. For additional specificity, FCPS DTI and ISOs, in accordance with NIST guidance, should leverage the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) for system specific security configuration requirements.

2.1. Critical Information Security (CIS) Controls

The FCPS DTI Information System Security Manual will detail the minimum-security process and control requirements for an approved and authorized information system, to a moderate level of detail. Other referenced resources, both government and industrial, are leveraged to provide system specific guidance at a granular level.

The FCPS WISP framework starts with an understanding of the twenty (20) controls, which should be implemented for establishing essential cyber security practices. The CIS Controls have been developed by SANS to be a prioritized set of activities aimed towards addressing the most common and pervasive attack methodologies. As a result, the following CIS Controls can be seen as a starting point for the implementation of a formal WISP.

Basic:

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers.
6. Maintenance, Monitoring, and Analysis of Audit Logs

Foundational:

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices; such as, Firewalls, Routers, and Switches, etc.

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

12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational:

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

3 Roles and Responsibilities

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

- Department of Technology Infrastructure (DTI)
- FCPS Departments
- Employees and Contractors
- Third-Party Services Vendors

Additionally, the following mandatory/key roles and responsibilities are included:

- Authorizing Official
- Director of Technology Infrastructure
- Information System Security Manager (ISSM)
- Information System Owner (ISO)
- Incident Response Team (IRT)

3.1. Department of Technology Infrastructure (DTI)

The Duties and Responsibilities of the DTI are:

- Provide IT Governance and oversight for all FCPS Departments and Information Systems
- Developing, maintaining, and revising IT procedures and standards
- Providing expert guidance, technical assistance, and recommendations to the FCPS BoE, the FCPS Superintendent, and the FCPS Chief Operating Officer (COO) concerning all IT matters

- Implement and maintain a Written Information Security Program (WISP)
- Determine the feasibility of conducting regular external and internal information systems data security audits, including vulnerability assessments and penetration testing to verify security controls are working properly and to identify weaknesses
- Archive security assessment results for a minimum of ten (10) years and make them available to DoIT upon request
- Assess the implementation of a risk management process for the life cycle of each critical IT system
- Assume the leading role in resolving FCPS security and privacy incidents, in accordance with FCPS Incident Response procedures
- Enforcing the guidelines established in Maryland State Government Article §10-13 Protection of Information by Government Agencies

3.2. FCPS Departments

Information Security is the responsibility of the FCPS Department. The department leadership must provide clear direction and visible support for security initiatives. The Duties and Responsibilities of FCPS Departments are:

- Initiate measures to assure and demonstrate compliance with the security requirements within this document
- Designate, for each security boundary, an ISO for implementing and maintaining the FCPS security program
    - The ISO will:
        - Classify data according to sensitivity
        - Approve access and permission to data
        - Ensure methods are in place to prevent and monitor inappropriate access to confidential data
        - Maintain the Records Management program for the system, including monitoring that retention and destruction policies are properly enforced
        - Ensure the fidelity of implementation for the all aspects of information system management, in accordance with the ATO Package documentation
- Ensure that security is part of the department's planning and procurement process
- Participate in annual information system data security self-audits, focusing on compliance with this document and the ATO Package
- Implement a risk management process for the life cycle of each critical IT system managed by the department
- Assure the confidentiality, integrity, availability, and accountability of all FCPS information, while it is being processed, stored, or transmitted electronically, and the security of the resources associated with those processing functions

- Assume a primary response role in resolving FCPS security and privacy incidents, in accordance with FCPS DTI Incident Response Procedures
- Abide by the guidelines established in Maryland State Government Article §10-13 Protection of Information by Government Agencies[2]
- Develop, implement, and annually test an IT Disaster Recovery Plan for IT systems in accordance with the security boundary's Contingency Plan/Disaster Recovery Plan (CP/DRP) guidelines
- Ensure separation of duties and assign appropriate systems permissions for IS users, in accordance with role based security doctrine and best practices
- Abide by the Records Management Guidelines established by the Maryland Department of General Services and the Maryland State Archives

3.3. Employees and Contractors

All FCPS Employees and Contractors are responsible for:

- Being aware of and complying with FCPS policies and regulations for the protection of IT Assets
- Using IT resources only for the intended purposes as defined by laws, policies, regulations, and operating procedures
- Being accountable for their actions relating to their use of all IT systems

3.4. Third-Party Services Vendors

A third-party service vendor is an organization, commercial or private, that offers/provides any third-party service offerings to FCPS (e.g. IaaS, PaaS, SaaS).

In accordance with Maryland State Government Article § 10-1304; FCPS must require, by contract or agreement, all third-party service providers receiving Confidential FCPS information, implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information disclosed to the third-party organization and are reasonably designed to help protect the information from unauthorized access, use, modification, disclosure, or destruction.

All third-party service vendors are responsible for meeting the requirements defined in this manual. Further detail regarding the division of responsibilities between FCPS and a third-party vendor can be found in the Cloud Computing Technologies and Vendor Risk Assessment sections of the FCPS DTI Information System Security Manual.

[2] Maryland State Government Article §10-13 Protection of Information by Government Agencies

Failure to consistently meet the security requirements defined herein, or otherwise legally or contractually applicable, will result in the termination of contracted services and may result in additional penalties.

3.5. Authorizing Official (AO)

The Authorizing Official (AO) formally assumes responsibility for operating the IS at an acceptable level of risk to organizational operations, organizational assets, individuals, and other organizations.

The Director of Technology Infrastructure is designated as the FCPS AO.

The following authorization decisions can be made by the AO:

- **Authorization to Operate (ATO)** – Full authorization may be granted when all 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 a production operating 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 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 DTI, 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 a production operating 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.

3.6. Director of Technology Infrastructure

The Director of Technology Infrastructure is responsible for FCPS's WISP.

The Director of Technology Infrastructure has the following IT Security responsibilities:

- Develop, maintain, and oversee the FCPS IT Security Program
- Monitor and report IT security program compliance to the FCPS BoE, Superintendent, and Chief Operating Officer
- Serve as the IT security liaison to DoIT and external organizations
- Ensure sufficient resources are available to implement the FCPS IT security program in coordination with FCPS other departments
- Ensure, in coordination with FCPS leadership, the implementation of the requirements of an organization-wide IT Security Program (as specified in § 3544, paragraph (b)[3], of the Federal Information Security Management Act (FISMA))
- Ensure that FCPS 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 FCPS leadership regarding their responsibilities for security
- Report on the status of the WISP to the FCPS Superintendent annually
- Brief FCPS Cabinet 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 system and if an information subsystem will adequately protect sensitive information
- Ensure FCPS IT security planning and execution is practiced throughout the life cycle of each FCPS IS
- Ensure FCPS 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

[3] https://csrc.nist.gov/CSRC/media/Projects/Risk-Management/documents/FISMA-final.pdf

- Ensure the security program is sufficiently staffed and funded to achieve its approved objectives in a timely manner
- Ensure that FCPS IT security policies and procedures are developed, approved and maintained in accordance with this Maryland IT Security Manual

3.7. Information System Security Manager (ISSM)

The ISSM is responsible for ensuring the implementation of FCPS's WISP.

The Supervisor of Infrastructure and Security or Designee is designated as the FCPS ISSM.

The ISSM has the following IT Security responsibilities:

- Facilitate the ISO's development, maintenance, and oversight of the FCPS WIPS within the assigned security boundary
- Monitor and report IT security program compliance to the Director of Technology Infrastructure
- Serve as the IT security liaison to FCPS Departments and ISOs.
- Ensure that all ISOs perform an evaluation of the WISP and its practices of the security boundary, at minimum annually (as specified in § 3545 of the FISMA)
- Assist and advise ISOs and FCPS Departments regarding their responsibilities for security
- Consult with and brief the Director of Technology Infrastructure regarding all critical information system security issues
- Ensure ISOs are identified and that security authorization for those resources are accomplished within the planned time-frame
- Ensure security boundaries and their subsystems are operating at an acceptable risk level, which will adequately protect sensitive information
- Review the security boundary ATO Package and sign documents that require ISSM signature
- Ensure FCPS IT security planning and execution is practiced throughout the life cycle of each security boundary
- Ensure that persons with IT security responsibilities have appropriate role-based training
- Assist oversight groups in compliance reviews and other reporting requirements

3.8. Information System Owner (ISO)

The Information System Owner (ISO) has development and operational responsibility for an FCPS IS within their assigned Information Security Boundary.

Multiple[4] Information System Owners can be designated as required; however, each IS must have at least one (1) assigned ISO. The ISO 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 FCPS 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 Plan, as defined in the ATO Package
- 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 the Risk Assessment Report (RAR) accordingly
- Develop and maintain the ATO Package for the security boundary
- Update the ATO Package 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
- Approve 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 FCPS guidelines upon personnel transfer, termination, or change in duties
- Ensure IS personnel are properly designated, monitored, and trained, including appointment in writing of an individual to serve as the Technical Lead (TL), if appropriate
- Inform the AO and ISSM of the need to conduct a security authorization effort and ensure that appropriate resources are available for the effort
- Coordinate with the ISSM 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 System Development Life Cycle (SDLC) process to protect the business operations and information the system supports
- Work with the ISSM to meet shared IT security responsibilities
- Ensure the security boundary Incident Response Team (IRT) is staffed, trained, and maintained in a state of readiness

[4] In the event multiple ISOs are assigned to a single security boundary, one (1) ISO must be listed as the primary or senior ISO.

- Ensure the security program for the security boundary is sufficiently staffed and funded to achieve its approved objectives in a timely manner

3.9. 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 FCPS IRT is designated by the Director of Technology Infrastructure. The ISO is responsible for designating the IRT representatives for their assigned security boundary.

In the event of an Incident, the IRT has the following additional IT Security responsibilities:

- Must ensure FCPS complies with specified security controls through operations standards contained in this manual
- Takes the necessary actions to alert the appropriate personnel of suspected intrusions to FCPS IS
- Analyze and document Information Security incidents and security events
- Perform investigations of potentially malicious or suspicious activity
- Receive and monitor security alerts and advisories from the United States Computer Emergency Readiness Team (US-CERT) and take appropriate action in response to alerts and advisories
- Report security incident information to the Director of Technology Infrastructure.
- Complete and submit the appropriate reports to non-FCPS entities (e.g. MD DoIT for a CAT 1 incident, FTI reports to the Treasury Inspector General for Tax Administration (TIGTA) and IRS Office of Safeguards, Criminal reports to Frederick County Police and the FBI)

4 Information Classification Guidelines

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

These guidelines pertain to all information within FCPS 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 these guidelines and educate users that may have access to confidential information for which they are responsible. All FCPS and Maryland State information is categorized into two main classifications with regard to disclosure:

- **Public Information** - is information that has been declared publicly available by FCPS or Maryland State officials with the explicit authority to do so and can freely be given to anyone without concern for potential impact to FCPS or 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 Information (PCI), Privileged or Sensitive, as defined below.

4.1. Personally Identifiable Information (PII)

The definition of PII varies depending if the subject is an adult or a student. However, the basic underlying principles are consistent. Laws and regulations governing the identification and protection of PII make a distinction between adult and student information. FCPS operates with two distinct categories of PII, Personally Identifiable Information – Adult (PII-A) and Student Information. As a result of the Family Education Rights and Privacy Act (FERPA), FCPS has further subdivided Student Information into Directory Information (DI), Limited Directory Information (LDI), and Student Personally Identifiable Information (SPII).

4.1.1. Personally Identifiable Information – Adult (PII-A)

The FCPS guidance for Personally Identifiable Information – Adult (PII-A) applies to all information collected or generated, while the subject is over the age of 18 years old and not an actively enrolled student with a K-12 Local Education Agency (LEA). FCPS adheres to the Federal definition of PII provided by the OMB.

The federal Office of Management and Budget (OMB) provides a definition, which applies to the core concept of PII:

Personally Identifiable Information (PII). The term "PII," as defined in OMB Memorandum M-07-1616 refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual.

The creation, storage, manipulation and sharing of PII-A information must always be conducted within the FCPS.org domain. This information may be shared between FCPS employees, with a legitimate need to know, using the file share system (e.g. H/K/R/U/V drives) or other secure FCPS provided and approved software (e.g. PeopleSoft). The information systems used to collect, store, and access PII-A must be listed in the Information System Security Inventory of PII & FCPS Confidential Data. The FCPS records containing PII-A must be listed in the Inventory of Records Containing PII & FCPS Confidential Data.

FCPS DTI is able to facilitate secure means to transfer PII-A internally and externally to individuals/organizations, who have a legitimate need to know. The Department of Technology Infrastructure is able to provide training and approval for these transfers upon request.

PII-A Information may be disclosed without written consent under the following conditions and via DTI approved means of communication:

- To FCPS officials with a legitimate need to know. This includes staff and legal agents, who require access in order to perform their official FCPS duties
- Disclosure to comply with judicial order or lawfully issued subpoena
- In the event of disclosure for a health/safety emergency, the nature of the emergency, what information was disclosed and to whom the information was released must be documented
- As otherwise required by federal or state law or regulation

4.1.2. Student Information Classification

The FCPS guidance, for the classification of student information, applies to all information collected or generated, while the subject is/was under the age of 18 years old and/or an enrolled student with a K-12 LEA.

FCPS, in accordance with FERPA, divides this information into three major categories; Directory Information (DI), Limited Directory Information (LDI), and Personally Identifiable Information (SPII).

4.1.2.1. Directory Information (DI)

The *Family Educational Rights and Privacy Act* (FERPA), a Federal law, requires that public schools, with certain exceptions, obtain written consent prior to the disclosure of personally identifiable information from a student's education records. However, FCPS may disclose appropriately designated "Directory Information" without written consent, unless the parent has advised the school to the contrary in accordance with FCPS procedures. The primary

purpose of directory information is to allow FCPS to include information from a student's education records in certain school publications.

Directory Information, which is information that is generally not considered harmful or an invasion of privacy if released, can also be disclosed to outside organizations without a parent's prior written consent. Outside organizations include, but are not limited to, companies that manufacture class rings or publish yearbooks. In addition, two federal laws require local educational agencies (LEAs) receiving assistance under the Elementary and Secondary Education Act of 1965, as amended (ESEA) to provide military recruiters, upon request, with the following information – names, addresses and telephone listings – unless parents have advised the LEA that they do not want their student's information disclosed without their prior written consent. **[Section 9528 of the ESEA (20 U.S.C. § 7908) and 10 U.S.C. § 503(c).]**

The following items are considered Directory Information and **may be disclosed without written consent**, per *Title 34 CFR Subtitle A Chapter I Part 99 Subpart D Section 99.*37:

- Student's Name
- FCPS Issued Email Address
- Field of Study
- Honor Roll Selection
- Degrees/Awards Received
- Dates of Attendance
- Photograph, Video or other electronic images
- Participation in officially recognized activities and sports
- Physical statistics (e.g. weight and height for athletic teams)
- Most recent school of attendance
- A playbill or other program showing student roles in drama or music productions

Parents who do not want Directory Information from their child's education records to be disclosed by their child's school, must notify the school in writing by September 30 or within 30 days of date of enrollment. However, a parent or eligible student may not opt out of the disclosure of DI in order to prevent a school from requiring a student to wear a student Identification badge that exhibits information that the school has properly designated as "Directory Information."

Items containing information considered to be DI, may be developed, store, and distributed without prior written consent. Individuals are required to use reasonable discretion and make a best effort to only share as much of this information as is necessary to accomplish the FCPS mission for which the information is being shared. This information may be worked upon in

FCPS provided Google accounts (e.g. G Suite for Education, Google Drive, Google Docs), FCPS support websites (e.g. www.fcps.org, official school website), or the FCPS.org domain (e.g. H: drive, K: drive, Outlook, Microsoft Office, SharePoint) environments.

4.1.2.2. Limited Directory Information (LDI)

Per 34 C.F.R. § 99.37(d), a school or school district may adopt a limited directory information policy. Limited Directory Information (LDI) **may be released to approved organizations**, unless specifically prohibited by the parent or eligible student.

- Parents and teachers
- School system in which a student seeks or intends to enroll
- Branch of the military
- Persons engaged by a school or board of education to confirm a home address or home phone number
- Law enforcement
- Emergency health services
- Post-secondary educational institution
- Maryland State or Federal Department of Education
- Maryland Higher Education Commission
- FCPS Authorized Representative

Release of LDI to any other person or entity is not permitted unless the release of the LDI is otherwise consistent with applicable law, FCPS policy and aligned with the educational mission of the district, as determined by the superintendent of schools or designee.

FCPS has defined LDI information as:

- FCPS Student ID
- Student's parent, guardian or other family member
- Graded Assignments
- Student's Address
- Phone Number
- Date of Birth
- Place of Birth
- Personally Obtained Email Address

LDI data may be developed and stored in any FCPS provided or approved systems (e.g. GAFE, FCPS.org domain). However, it is the responsibility of the data owner to ensure the information is ONLY shared with approved individuals/organizations, who have a legitimate educational

interest. FCPS must receive prior written consent, from a parent/guardian or eligible student, to share LDI information with any non-enumerated recipient. Any incident in which LDI is shared with sources, other than those listed, must be reported to the Department of Technology Infrastructure immediately.

4.1.2.3. Student Personally Identifiable Information (SPII)

Student Personally Identifiable Information (SPII) includes any record (digital or physical) maintained by FCPS that contains information that, alone or in combination, would make it possible to identify an individual with reasonable certainty (electronic or physical). These items **may not be disclosed** outside of FCPS without express written consent of a parent/guardian or eligible student or in accordance with *Title 34 CFR Subtitle A Chapter I Part 99 Subpart D Section 99.*31. If uncertain, always assume information is SPII and seek further clarification.

SPII records include:

- Social Security Numbers
- Biometric Record
- Residence Status
- Religious preferences
- Grades of Record
- Test Results
- Academic Transcripts
- Course Schedule
- Student Evaluations
- Socioeconomic Information
- Food Purchases
- Disciplinary Records
- Special Education Records
- Student Financial Records
- Employment Records
- Health Records
- FCPS Technology Activity Reports

The creation, storage, manipulation and sharing of SPII information must always be conducted within the FCPS.org domain. This information may be shared between FCPS employees, with a legitimate educational interest, using the file share system (e.g. H/K/R/U/V drives) or other secure FCPS provided and approved software (e.g. eSchool, 504 Portal). The information

systems used to collect, store, and access SPII must be listed in the *Information System Security Inventory of PII & FCPS Sensitive Data*. The FCPS records containing SPII must be listed in the *Inventory of Records Containing PII & FCPS Sensitive Data*.

FCPS DTI is able to facilitate secure means to transfer SPII internally and externally to individuals/organizations, who have a legitimate educational need. The Department of Technology Infrastructure is able to provide training and approval for these transfers upon request.

SPII Information may be disclosed without written consent under the following conditions and via DTI approved means of communication:

- To FCPS officials with a legitimate educational interest. This includes staff and legal agents, who require access in order to perform their official, educationally-related duties.
- Disclosure to accrediting organizations or FCPS approved organizations conducting studies to improve educational instruction.
- Disclosure to comply with judicial order or lawfully issued subpoena.
- In the event of disclosure for a health/safety emergency, the nature of the emergency, what information was disclosed and to whom the information was released must be documented.
- As otherwise permitted by federal or state law or regulation

4.2. Federal Tax Information (FTI)

Federal Tax Information (FTI) includes tax return or tax 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. According to IRS Publication 1075, the security framework defined by NIST SP 800-53 moderate-level security controls provide the requirements necessary for protecting information systems that receive, process, store, or transmit FTI. A crosswalk of FTI security controls to the NIST standards contained in this manual, is available in the IRS Publication 1075.

4.3. Protected Health Information (PHI)

Protected Health Information (PHI) is health data created, received, stored, or transmitted by FCPS and their associated entities 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. PHI information is governed in accordance with the requirements prescribed by the Health Insurance Portability and Accountability Act (HIPAA). FCPS information systems that store, process, and/or transmit this data type must comply with the Health Insurance Portability and Accountability Act (HIPAA) control requirements (CFR Title 45 - Subtitle A - Subpart C - Part 164) to ensure reasonable administrative, technical, and physical safeguards are in place to prevent intentional or unintentional use or disclosure of PHI. The U.S. Department of Health & Human Services HIPAA Security Rule requirements are covered, in the majority, by organizations compliant with the NIST Cybersecurity framework; however, potential gaps may be identified, which need to be addressed directly.

A crosswalk of PHI security controls to the NIST standards contained in this manual, is available in Appendix C.

4.4. Payment Card Information (PCI)

Payment Card Information (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. The PCI Security Standards Council (PCI SSC) has documented the use of the NIST Framework to meet PCI compliance requirements.

A crosswalk of PCI DSS security controls to the NIST standards contained in this manual, is available in Appendix D.

4.5. 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 FCPS or by any person working for FCPS;

- Provided by any other Maryland or Frederick County agency to FCPS in the course of FCPS's exercise of its responsibility to prepare and monitor the execution of the annual budget;
- Relating to FCPS 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 FCPS 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)

4.6. Sensitive

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

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 appropriate handling guidelines.

4.6.1. Persistent Organizational Purpose

Any FCPS information or digital resource, regardless of information classification, used for a persistent organizational purpose should reside on the FCPS network or an FCPS authorized third-party system, specifically approved for the purpose the information is collected to fulfill. The use of Google (e.g. drive, sheets, sites, etc.), DropBox, Weebly, Wix, or other like services, to fulfill persistent organizational purposes, is prohibited, unless explicit permission is received from the Director of Technology Infrastructure.

5 Guidelines for Marking and Handling FCPS-Owned Information

It is necessary to classify and mark 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 FCPS systems: No restrictions
- Distribution outside of FCPS 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 information 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 FCPS and Maryland state employees or contractors with explicit need-to know and other individuals for whom an authorized FCPS official has determined there is a need-to-know and an appropriate non-disclosure agreement has been obtained
- Distribution within FCPS systems; Delivered direct - signature required, envelopes stamped Confidential, or an approved, electronic email or electronic file transmission method
- Distribution outside of FCPS 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 the Director of Technology Infrastructure (or delegated authority) has been granted. Approved storage on portable devices or publicly accessible systems must be encrypted; kept 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 and record the action, in accordance with the appropriate Records Management Retention Schedule on file with the Maryland State Archives. Disposal of paper information by shredding the document; 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-FCPS owned devices unless prior written approval from the Director of Technology

Infrastructure (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 algorithms compliant with NIST 800-52 Revision 2 and 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.

6 System Security Categorization Procedures

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 information system's security level, within the system Security Categorization (SecCat) artifact of the ATO Package, helps to determine the level of effort or controls required to protect it.

This requirement applies to all information systems within FCPS. Department officials must use the security categorizations described in this manual and supplemented by 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 the DTI's discretion.

The security categories are based on the potential impact to FCPS should certain events occur which jeopardize the information and information systems needed by FCPS to accomplish its 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 FCPS.

6.1. Security Objectives

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

Confidentiality:

Confidentiality refers to preventing the disclosure of information to unauthorized individuals or systems.

For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, etc.), and by restricting access to the places where the data is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred.

Confidentiality is necessary for maintaining the privacy of the people whose personal information a system holds.

- "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:

In information security, data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle. This means that data cannot be modified in an unauthorized or undetected manner. This is not the same thing as referential integrity in databases, although it can be viewed as a special case of Consistency, as understood in the classic ACID (Atomicity, Consistency, Isolation, Durability) model of transaction processing.

Integrity is violated when a data is modified by an unapproved source, while in-transit or at-rest.

- "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:

For any information system to serve it purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls needed to protect it, and the communication Channels used to access it, must be functioning correctly. The availability of an information system aims to meet the service level expectation set by its mission and function. Ensuring availability involves activities, which may or may not seem directly related to the information system. For example, preventing power disruptions, preventive measures for hardware operational and support failures (e.g. life cycle replacement planning), system upgrades (e.g. patch management), protections against denial-of-service attacks, etc.

- "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

6.2. Potential Impact on the Organization or Individuals

The MD DoIT IT Security Manual and FIPS Publication 199 define 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 FCPS and overall State interest.

6.2.1. "LOW" Potential Impact

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.

6.2.2. "MODERATE" Potential Impact

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.

6.2.3. "HIGH" Potential Impact

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.

6.2.4. "LOW" vs "MODERATE"/"HIGH" Checklist

Table I is a checklist to help determine the categorization of an FCPS IS. If any of the following are marked as true, the IS should not be categorized as "Low" and a "Moderate" or "High" classification is likely.

6.2.4.1. Table I – "LOW" vs "MODERATE"/"HIGH" Checklist

Question/Criteria	Yes	No
Is there the possibility for citizens' names, addresses, age, workplace, student address, and/or any biometric information, or any other Confidential Classification of 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?		

6.3. Security Categorization Applied to FCPS 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.

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

6.3.1. FCPS SecCat Modifier

Through the process of risk determination, FCPS DTI may classify an Information Security Boundary as an FCPS "Critical" system due to mission criticality or sensitive criteria. As an FCPS "Critical" security boundary, additional control requirements from the High category or other source, may be mandated for ATO compliance.

7 Asset Management

All major information systems asset must be accounted for and have a named ISO. Accountability for assets helps to ensure that appropriate protection is maintained. Information system owners must be identified for all major assets and the responsibility for the maintenance of appropriate controls must be assigned. Responsibility for asset accountability may be delegated via the FCPS Property Issued Form. However, the responsibility of ensuring the implementation of security controls and ultimate asset accountability must remain with the named Information System Owner of the asset.

All FCPS Information Technology Assets must be tagged and tracked via the FCPS DTI Technology Inventory Management System, in accordance with the appropriate policies, regulations, and procedures.

7.1. Inventory of Assets

Compiling an inventory of assets is an important aspect of risk management. FCPS needs to be able to identify the assets and the relative values and importance of these assets. Based on this information, FCPS can then provide appropriate levels of protection. Inventories of the important assets associated with each information system should be documented and maintained by the system ISO within the ATO Package identified accountability resource. Asset inventories must include; a unique system name, an ISO, 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
- Services: computing and communications services, general utilities (e.g., heating, lighting, power, air-conditioning)

8 Security Control Requirements

This section defines requirements that must be met for FCPS to properly protect confidential information under FCPS's administrative control. All information systems (hosted on the FCPS 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 *State of Maryland Information Technology Security Manual version 1.2*, *NIST SP 800-30 Risk Management Guide for Information Technology Systems* and *NIST SP 800-53, Recommended Security Controls for Federal Information System*s and also the *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 (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems*, are included in this manual as a baseline.

Systems with a "HIGH" category level should consult the DTI and 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

The controls enumerated in this manual provide the minimum Management, Operational, and Technical level controls required for all FCPS information systems. However, different types of systems require system specific controls to be put in place. FCPS DTI leverages the Security Technical Implementation Guides (STIGs), published by the Defense Information Systems Agency (DISA), to provide system specific security configuration requirements.

8.1. Management Level Controls

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.

8.1.1. 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 organization to successfully implement and maintain an acceptable level of security. A risk management process must be implemented to assess the acceptable risk to FCPS IT systems as part of a risk-based approach used to determine adequate security for FCPS 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. FCPS 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. The DTI employs the *NIST SP 800-30 (R1) Guide for Conducting Risk Assessments* framework as a basis 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 WISP requirements. The controls presented in the Security Controls Compliance Matrix section of this document are designed to mitigate risks and are required to be compliant with the FCPS security program.

The third process of risk management, evaluation, is ongoing and evolving. Evaluation emphasizes the good practice to develop an effective risk management program within FCPS's information security program. Not only should the risk management program drive changes to existing systems, but it should also integrate into FCPS's operational functions, as well as the SDLC for new systems and applications. Section 12.5.1.1 outlines the minimum security control requirements, which all FCPS information systems must adhere to in order to operate in a production environment.

8.1.2. Security Assessment and Authorization

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

Custodians of confidential information (ISOs) will, via the completion and submission of the ATO Package, 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. FCPS AO must approve, sign, and issue the ATO Memo.

ISOs must continuously (at least annually) monitor the security controls within their information systems to ensure that the controls are operating as intended. The ISSM must authorize and the ISO must document all connections from information systems to other information systems outside of the system boundary using Interconnection Security Agreements and monitor/control system connections on an ongoing basis.

FCPS 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. ISOs 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 POA&M 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 POA&M and the CAP must address implementation of security controls to reduce or eliminate known vulnerabilities in agency systems. Section 12.5.1.2 outlines the minimum-security control

requirements, which all FCPS information systems must adhere to in order to operate in a production environment.

8.1.3. Planning

FCPS security planning controls include system security plans (SSP) and system security plan updates. The ISO 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 FCPS 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 (Appendix A)
- System Authorization (ATO Memo)
- Security training, awareness, and education

When the 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 as 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 and those performing system management functions to general users, have received security training at levels commensurate with the duties they perform. Section 12.5.1.3 outlines the minimum-security control requirements, which all FCPS information systems must adhere to in order to operate in a production environment.

8.1.4. Program Management

The Program Management (PM) control family applies to the implementation of the FCPS cybersecurity program. It includes a critical infrastructure plan, information security program plan, a plan of action milestones and processes, a risk management strategy, and enterprise architecture.

8.2. Operational Level Controls

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.

8.2.1. Awareness and Training

FCPS must ensure all information system users and managers are knowledgeable of security awareness material before authorizing access to systems. FCPS must also 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. FCPS must document and monitor individual information system security training activities including basic security awareness training and specific information system security training. Section 12.5.2.1 outlines the minimum-security control requirements, which all FCPS information systems must adhere to in order to operate in a production environment.

8.2.2. 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). ISOs 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 to perform the responsibilities of the organizational role
- 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 FCPS 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. Section 12.5.2.2 outlines the minimum-security control requirements, which all FCPS information systems must adhere to in order to operate in a production environment.

8.2.3. Contingency Plan / Disaster Recovery Plan

FCPS 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 provide a foundation for a systematic and orderly resumption of all computing services within FCPS when disaster strikes.

Primary Components of a 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) in the Contingency Test Plan
- Identification of disaster recovery site including contact information
- System Recovery Time Objective (RTO)
- System Recovery Point Objective (RPO) (how current should the data be?)
- Procedures for system restoration at backup and original FCPS site

Section 12.5.2.3 outlines the minimum-security control requirements, which all FCPS information systems must adhere to in order to operate in a production environment.

8.2.4. Incident Response

Information Technology Incident Management refers to the processes and procedures FCPS implements for identifying, responding to, and managing information security incidents. A computer incident within Maryland is defined as a violation of computer security policies, acceptable use policies, or standard computer security practices. Refer to FCPS Regulation 200-31, DTI Data Breach Incident Response Process, and NIST SP 800-61 Revision 2 Computer Security Incident Handling Guide for guidance in creating an Incident Response Plan and procedures to support it.

To clearly communicate incidents and events (any observable occurrence in a network or system), it is necessary for the FCPS incident response teams to adopt a common set of terms and relationships between those terms. All elements of FCPS should use a common taxonomy, per the definitions of terms, roles, and procedures contained in the Incident Response Plan. ISOs and the ISSM 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. 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.

FCPS must report all CAT 1 IT incidents to DoIT and the Maryland State Chief Information Security Officer (CISO) by completing an IT Incident Report (Appendix B) 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 FCPS, and the final resolution. Section 12.5.2.4 outlines the minimum-security control requirements, which all FCPS information systems must adhere to in order to operate in a production environment.

8.2.5. 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. FCPS 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. The designated ISO must ensure that system maintenance is scheduled, performed, and documented, for the

security boundary, in accordance with manufacturer or vendor specifications and/or FCPS DTI requirements. Only authorized personnel are to perform maintenance on information systems. Section 12.5.2.5 outlines the minimum-security control requirements, which all FCPS information systems must adhere to in order to operate in a production environment.

8.2.6. Media Protection

The purpose of Media Protection 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". FCPS must restrict access to system media containing confidential information to authorized individuals.

Media labeled "Confidential" must be physically controlled and securely stored. FCPS 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.

FCPS should 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 DTI designated software and protected consistent with the classification of the data.

Throughout the lifecycle of IT equipment, there are times when an FCPS department 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 trade-in, lease termination, or disposal. 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 FCPS data, FCPS 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 FCPS'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 FCPS. Section 12.5.2.6 outlines the minimum-security

control requirements, which all FCPS information systems must adhere to in order to operate in a production environment.

8.2.7. 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
- Operations and control areas

FCPS 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
- Ensuring that any physical access controls are auditable
- Ensuring that employees/contractors receive annual training regarding physical security best practices

Section 12.5.2.7 outlines the minimum-security control requirements, which all FCPS information systems must adhere to in order to operate in a production environment.

8.2.8. Personnel Security

Personnel Security (PS) controls establish standards around personnel screening, termination, transfers, sanctions, and access agreements are all examples of PS controls to protect employees. These controls are limited to the minimum-security controls from an information and cyber security standpoint. Additional personnel security standards and requirements are maintained by the FCPS offices of Security & Emergency Management and Human Resources.

8.2.9. Supply Chain Risk Management

Supply Chain Risk Management (SCRM) control family and integrates supply chain risk management aspects throughout the other control families to help protect system

components, products, and services that are part of critical systems and infrastructures. The SCRM controls help ensure that security and privacy requirements, threats, and other concerns are addressed throughout the system development life cycle and the national and international supply chains.

8.2.10. System and Information Integrity

FCPS 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 ISOs 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 FCPS DTI requirements. Section 12.5.2.8 outlines the minimum-security control requirements, which all FCPS information systems must adhere to in order to operate in a production environment.

8.2.11. System and Services Acquisition

FCPS must develop, document, and disseminate a system and services acquisition process that addresses purpose, scope, roles, responsibilities, management commitment, coordination amongst internal entities, and enforce compliance. The procedures and controls to facilitate the implementation of the system and services acquisition process must also be developed, documented, and disseminated.

These controls address the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. However, this is not guaranteed, requiring each ISO to evaluate the policies, regulations, and procedures as they apply to the assigned security boundary.

8.3. Technical Level Controls

Technical security controls focus on functions 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.

8.3.1. 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

Section 12.5.3.1 outlines the minimum-security control requirements, which all FCPS information systems must adhere to in order to operate in a production environment.

8.3.2. 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 ISSM, ISO, FCPS DTI, 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. Section 12.5.3.2 outlines the minimum-security control requirements, which all FCPS information systems must adhere to in order to operate in a production environment.

8.3.3. Identification and Authorization Control Requirements

Identification and authorization are technical measures that prevent 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 FCPS systems must have a means to

enforce user accountability when using FCPS IT systems, so that system activity (both authorized and unauthorized) can be traced to specific users. To ensure user accountability, FCPS requires that all 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. User identification and authentication also can enforce separation of duties.

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). Multifactor authentication requires two separate factors for system access (e.g. smartcard (have) and PIN (know)). FCPS information systems must implement systems capable of Single Sign-On (SSO) integration with valid FCPS DTI SSO services. FCPS Information systems should implement multifactor authentication using a FCPS DTI approved token for user network access.

Any FCPS system deviating from the FCPS SSO or Multifactor standard, must document an approved deviation from this control. The minimum standard, for AO deviation approval, consists of an individual identifier (e.g. username) and one factor of authentication (e.g. complex password).

Section 12.5.3.3 outlines the minimum-security control requirements, which all FCPS information systems must adhere to in order to operate in a production environment.

8.3.4. System and Communications Control Requirements

The System and Communications Protection control family describes the technical mechanisms that an information security boundary 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. Section 12.5.3.4 outlines the minimum-security control requirements, which all FCPS information systems must adhere to in order to operate in a production environment.

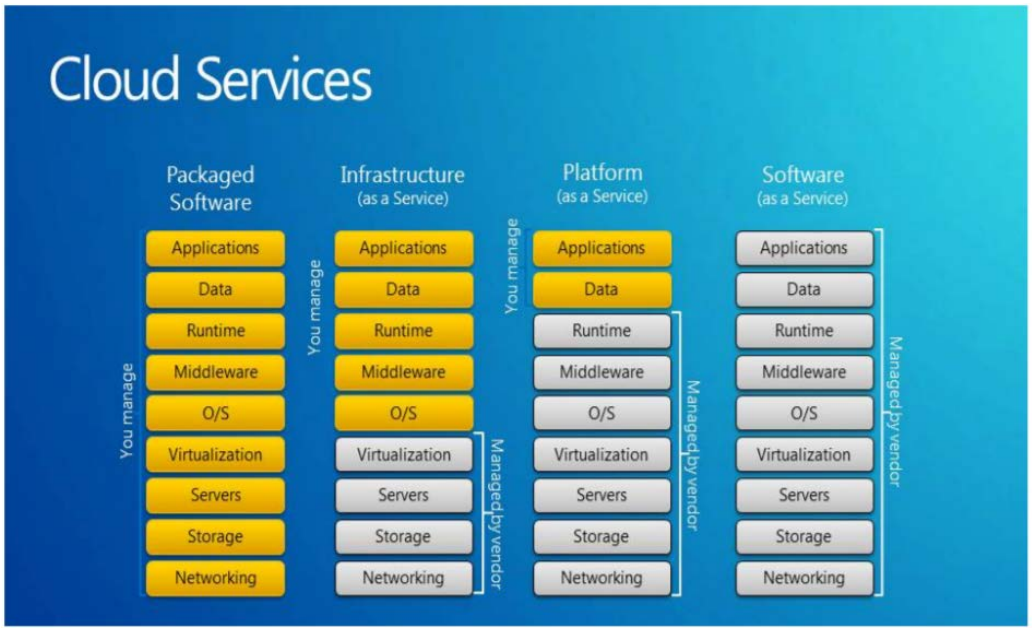
8.3.5. Virtualization Technologies

FCPS 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 FCPS 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 and NIST SP 800-125A Security Recommendations for Hypervisor Deployment must be adopted as the FCPS standard for securing virtualization solutions.

8.3.6. 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 FCPS 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 manual, in addition to any federal regulations that may apply.



As depicted in the Cloud Services diagram from the *DISA Risk Management, Cybersecurity Standards, Cloud Computing SRG v1r3*, each type of cloud service involves the transference of some FCPS responsibility for security control and management to an external entity. However, the accountability for the fidelity security implementation of FCPS information systems is never transferable to another entity (internal or external). The information system owner is always ultimately responsible for ensuring the risk remains at acceptable levels and security is consistently applied in accordance with the security boundary's Authorization to Operate documentation.

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 FCPS should consider when outsourcing data, applications and infrastructure to a public cloud environment. FCPS must adopt the security recommendations and guidelines described in SP 800- 144. The key guidelines to follow should 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 full 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

8.3.7. 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.

FCPS business requirements may, on occasion, justify storing confidential data on mobile computing devices. In these cases, FCPS is required to assure that steps have been taken to keep the data secure. It is the responsibility of FCPS 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 FCPS 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
- Whenever possible, mobile devices must be scanned for viruses/malware before they can connect to FCPS systems

The physical security of FCPS 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.

8.3.8. Data Loss Prevention Guidance

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

8.3.9. Privacy Controls

The privacy controls facilitate FCPS'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 Security Manual are primarily for use by FCPS's Director of Technology Infrastructure, when working with program managers, mission/business owners, ISOs, ISSMs, Department Leadership, information system developers/integrators, and risk executives to determine how best to incorporate effective privacy protections and practices (e.g., privacy controls) within FCPS programs and information systems and the environments in which they operate. Departments working with data governed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) should have an identified Privacy Officer (PO).

FCPS information systems 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 Departments and DTI to determine the information practices that are compliant with law and policy and those that may need review. It also enables FCPS 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 FCPS information Systems should strive to achieve but are not mandatory. FCPS DTI will decide when to apply control enhancements to support organizations particular mission/business functions.

8.3.9.1. Authority and Purpose

This control family ensures the identification of the legal basis that authorizes collection of PII or activity which may impact privacy. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. This family outlines the purpose(s) for which the data is being collected. Section 12.5.3.5.1 outlines the minimum-security control requirements, which all FCPS information systems must adhere to in order to operate in a production environment.

8.3.9.2. Accountability, Audit, and Risk Management

The accountability, audit and risk management privacy controls provide an overview of the governance, monitoring, risk management, and assessment used within FCPS and the state of Maryland. Implementing these controls demonstrates compliance with applicable privacy protection requirements and minimize the overall risk to managing privacy. Section 12.5.3.5.2 outlines the minimum-security control requirements, which all FCPS information systems must adhere to in order to operate in a production environment.

8.3.9.3. Data Quality and Integrity

This control family ensures that PII, which is collected and maintained by FCPS, is accurate, relevant, timely, and complete for the purpose for which it is to be used. Personal data should also be specifically relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date. Under the Family Educational Rights and Privacy Act (FERPA), parents and eligible students have the express right to inspect, review, and request corrections to educational records maintained by FCPS. Section 12.5.3.5.3 outlines the minimum-security control requirements, which all FCPS information systems must adhere to in order to operate in a production environment.

8.3.9.4. Data Minimization and Retention

Data minimization and retention controls require FCPS to collect, use, and retain only relevant PII necessary for the original purpose for which it was collected. The access, use, and sharing of FCPS data should be limited to the least possible quantity necessary to complete the legitimate educational or business requirement of FCPS. Data processing should only use as much data as is required to successfully accomplish a given task. Section 12.5.3.5.4 outlines the minimum-security control requirements, which all FCPS information systems must adhere to in order to operate in a production environment.

8.3.9.5. Individual Participation and Redress

This control family addresses the establishment of policy and procedures for the effective implementation of the controls and control enhancements in the Individual Participation and

Redress areas. An individual should be afforded the right to obtain from FCPS, or otherwise, receive confirmation of whether or not FCPS has data relating to the individual. The purpose for which personal data are collected, should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes. Data collected for one purpose, cannot be repurposed without further consent. Section 12.5.3.5.4 outlines the minimum-security control requirements, which all FCPS information systems must adhere to in order to operate in a production environment.

8.3.9.6. Privacy Security

Personal data should be protected by reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification, or disclosure of data. The privacy security section supplements the basic controls ensuring that technical, physical, and administrative safeguards are in place to protect personally identifiable information (PII) collected or maintained by FCPS. Section 12.5.3.5.5 outlines the minimum-security control requirements, which all FCPS information systems must adhere to in order to operate in a production environment.

8.3.9.7. Transparency

This family ensures that FCPS provide public notice of information practices and the privacy impact of programs and activities. FCPS should be open and transparent about developments, practices, and policies with respect to personal data. The means should be readily available to establish the existence and nature of personal data, and the main purposes of their collection, as well as the identity and role of the FCPS information owner. Section 12.5.3.5.6 outlines the minimum-security control requirements, which all FCPS information systems must adhere to in order to operate in a production environment.

8.3.9.8. Personally Identifiable Information (PII) and Transparency

The PII Processing and Transparency family of controls helps to safeguard sensitive data, focusing on consent and privacy. FCPS can lower the risk of data breaches by properly managing personally identifiable information.

8.3.9.9. Use Limitation

These controls ensure that FCPS only uses personally identifiable information (PII), either as specified in public notices, in a manner compatible with those specified purposes, or as otherwise permitted by law. Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified through the appropriately defined purpose, in accordance with the reasons given to receive the data subject's consent, or by the authority of law. Implementation of the controls in this family will ensure that the scope of PII use is limited accordingly. Section 12.5.3.5.7 outlines the minimum-security control

requirements, which all FCPS information systems must adhere to in order to operate in a production environment.

9 Information System Security Required Artifacts

An FCPS Department ISO must submit sufficient documentation in order for the AO to make a determination granting an ATO, ATO with Conditions, IATT, or DATO for an information system. The collection of documents required for consideration are collectively referred to as the Authority to Operate (ATO) Package (list provided in Table II – ATO Package Checklist).

9.1. Authorization to Operate (ATO) Package

In order to receive an Authorization to Operate (ATO) memo from the Director of Technology Infrastructure, the Information System Owners (ISO) will maintain an up-to-date ATO Package for submission, approval, and periodic review. ISOs are to review and update the ATO Package annually. In the event of a substantive system change, an updated ATO Package must be submitted and a new ATO memo issued, prior to change implementation.

It is recognized that security boundary Change Control Boards are empowered to approve potentially significantly impactful changes, which would require an update to security documentation; however, may not meet the threshold necessary for completing an entirely new ATO submission for AO approval. In these circumstances, the ISO must ensure the change documented in the Change Control Log, a Security Impact Analysis has been completed and signed by the security boundary's ISSM, and the appropriate ATO Package documents are updated. A non-comprehensive list of change examples requiring a documented Security Impact Analysis in lieu of a new ATO are provided in the table below.

#	Name	Condition
A	Device Configuration Standard	A new configuration standard is created for a device type (e.g. workstation, server, router)
B	Operating System Configuration Standard	A new configuration standard is created for an operating system.
C	Application Configuration Standard	A new configuration standard is created for an application.
D	Non-Configuration Deployment	A device, operating system, or application is deployed in a manner that is known to be non-conformant with baseline configuration standards.

9.1.1. Table II – ATO Package Checklist

(Artifacts labeled with "(I/A)" are required if determined to be applicable)

Documentation Title	Acronym	I/A	Status
Authorization to Operate (ATO) Memo	ATO Memo	Required	
Business Impact Analysis	BIA	Required	
Configuration Management Plan	CMP	Required	
System Baseline Configuration		Required	
Maintenance Plan	MA	Required	
Security Impact Analysis	SIA	Required	
Change Control Log	CCL	Required	
Maintenance Log		Required	
Contingency Plan / Disaster Recovery Plan	CP/DRP	Required	
Contingency Test Plan		Required	
Contingency Test Report		Required	
AO-Approved Deviation/Waiver Log		I/A	
Incident Response Plan		Required	
Interconnection Security Agreement	ISA	I/A	
Memorandum of Understanding/Agreement	MOU/A	I/A	
Service Level Agreement	SLA	I/A	
Vendor Contracts		I/A	
Plan of Action and Milestones	POA&M	Required	
Corrective Action Plan	CAP	I/A	
Privacy Impact Assessment	PIA	Required	
Privacy Threshold Analysis	PTA	I/A	
Records Management Plan	RM Plan	Required	
Security Assessment Plan	SAP	Required	
Risk Assessment Report	RAR	I/A	
Security Awareness and Training Plan		Required	
System Architecture Document	SAD	Required	
Information Security Architecture		Required	
Network Diagrams		Required	
System Inventory		Required	
Hardware Inventory		Required	
Software Inventory		Required	
Information Inventory (PII & Confidential)		Required	
System Security Categorization	SecCat	Required	
System Security Plan	SSP	Required	
System Specific Policies and Procedures		Required	
Media Protection Procedures		Required	
Physical and Environmental Protection Procedure		Required	
System and Information Integrity Procedure		Required	

Access Control Procedure		Required	
Audit and Accountability Control Procedure		Required	
Identification and Authorization Procedure		Required	
System and Communications Protection Procedure		Required	

9.1.2. Authorization to Operate (ATO) Memo

Memo issued by the AO authorizing the system to operate. The failure of an ISO to maintain system operations within the documented parameters established upon issuance of the ATO will result in the revocation of the system's ATO and the immediate termination of operations, until such a time as the system is brought back into compliance.

9.1.3. Business Impact Analysis (BIA)

The BIA documents specific system components, the critical services that they provide, and consequences of a disruption to the system and organizational components.

9.1.4. Configuration Management Plan (CMP)

Configuration Management (CM) is the disciplined approach to managing and controlling the evolution of the system development and maintenance. It enables the controlled and repeatable development, testing, release, and maintenance of the system's design artifacts, new hardware, and software components as they change over time. The Change Management Plan (CMP) establishes a standard CM process and authorizes the system's Change Control Board. The Change Advisory Board (CAB) monitors, approves, and tracks changes to the system's baseline configuration.

9.1.4.1. System Baseline Configuration

A baseline configuration provides information about the components of a system (e.g., the standard software load for a workstation, server, network component, or mobile device including the operating system and installed applications with current version numbers and patch information), the network topology, and the logical placement of the component within the system architecture. Baseline configurations serve as a reference point for future builds, releases, and/or changes to systems; therefore, they are required to effectively manage and secure system components as systems evolve and change over time.

9.1.4.2. Maintenance Plan

Maintenance Plan identifies, approves, controls, and monitors the use of information system maintenance tools and remotely executed maintenance and diagnostic activities on a regular

basis. The Maintenance Plan ensures that system maintenance is scheduled, performed, and documented, for the security boundary, in accordance with manufacturer or vendor specifications and/or FCPS DTI requirements.

9.1.4.3. Security Impact Analysis (SIA) Documentation (I/A)

A Security Impact Analysis (SIA) is an analysis conducted, by a member of the Change Control Board before implementing a change, to determine potential impact to the security state of the system.

9.1.4.4. Change Control Log

The Change Control Log is a continuous document, maintained by the CAB, which documents all approved changes to the baseline configuration and their completion status.

9.1.4.5. Maintenance Log

The Maintenance Log records the maintenance and diagnostic activities performed on FCPS information systems. The Maintenance Log documents the scheduled and performed system maintenance, for the security boundary, in accordance with manufacturer or vendor specifications and/or FCPS DTI requirements.

9.1.5. Contingency Plan / Disaster Recovery Plan (CP/DRP)

The Contingency Plan / Disaster Recovery Plan documents essential missions, business functions and associated contingency requirements, recovery objectives, restoration priorities and metrics, contingency roles and responsibilities, assigned individuals with contact information, procedures for maintaining essential missions and business functions affected as a result of an information system disruption, and procedures for full information system restoration without deterioration of the security measures originally planned and implemented. The CP/DRP must be tested at least annually. CP/DRP test cases must be documented in the Contingency Test Plan and the results of the test recorded in the Contingency Test Report.

The ISO shall develop a contingency planning capability to meet the needs of supporting critical operations in the event of a disruption. The procedures for execution of such a capability shall be documented in a formal information system CP/DRP and shall be reviewed, tested, and exercised at least annually and updated as necessary. Personnel responsible for target systems shall be trained to execute contingency procedures. The plan, recovery capabilities, and personnel shall be tested to identify weaknesses of the capability at least annually. The ISO shall ensure implementation of a Disaster Recovery Plan, including backup and restoration procedures for the designated security boundary. Components shall ensure the capability to re-

image information system components from configuration controlled and integrity protected disk images representing a secure, operation state for the components.

9.1.5.1. Contingency Test Plan

A Contingency Test Plan describes the type of tests and the methodology that will be used to test a DRP. It outlines which components will be tested during the test, as well as the details of what the test will entail. The results of the contingency test are documented in the Contingency Test Report.

9.1.5.2. Contingency Test Report

The Contingency Test Report documents the results of the Contingency Test Plan, any required action items and the period for resolving the items. During the system assessment, the team must review the action items, and determine whether the action items documented in the report have been addressed within the specific timeframe.

9.1.6. AO-Approved Deviation/Waiver Log (I/A)

The documented and approved deviation/waiver requests, within the AO-Approved Deviation/Waiver Log, are annually review by the ISO to verify the documented mitigating factors and compensating controls are in place, functioning as expected, and delivering desired results. The deviations are assessed to determine whether the risk of unmitigated weaknesses continues to be consistent with FCPS's evolving risk tolerance levels.

9.1.7. Incident Response Plan

An incident response plan defines what constitutes a security incident, for the ISO's security boundary, and outlines the incident response phases. It discusses how information is passed to the appropriate personnel, an assessment of the incident, minimizing damage and response strategy, documentation, and preservation of evidence. The incident response plan defines areas of responsibility and establishes procedures for handling various security incidents.

9.1.8. Interconnection Security Agreement (ISA) (I/A)

An Interconnection Security Agreement (ISA) specifies the technical and security requirements for establishing, operating, securing, and maintaining the interconnection between two systems operated by different organizations that were authorized to operate by different Authorizing Officials.

External network connections may be permitted only after all approvals are obtained consistent with this Manual and must be managed in accordance with an Interconnection Security

Agreement (ISA) that is agreed to by FCPS and the untrusted entity. Specific criteria should be included in the ISA regarding the system IT Security.

An ISA 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 FCPS and untrusted entities
- Roles and responsibilities of points-of-contact and cognizant officials for both FCPS and untrusted entities
- Security measures to be implemented by the untrusted organization to protect the FCPS's IT assets against unauthorized use or exploitation of the external network connection
- Requirements for notifying a specified FCPS official within a specified period (4 hours recommended) of a security incident on the network
- The *FCPS Data Collection Inventory* documentation
- The *FCPS Data Sharing Disclosure* documentation

9.1.8.1. Memorandum of Understanding/Agreement (MOU/A) (I/A)

A Memorandum of Understanding/Agreement (MOU/A) is a legal document describing an agreement between organizations establishing information security requirements and the terms and conditions of system interconnections.

9.1.8.2. Service Level Agreement (SLA) (I/A)

The Service Level Agreement (SLA) is the formal, signed agreement between organizations (e.g., system owners, system owner and application owner, etc.) documenting services provided by one party to the other for their system. SLAs must detail the roles and responsibilities required of each party and define the services provided, including services addressing security controls.

9.1.8.3. Vendor Contracts (I/A)

All legal agreements and/or contracts between FCPS and vendors delivering services within the defined security boundary.

9.1.9. Plan of Action and Milestones (POA&M)

The system vulnerabilities enumerated through secure implementation of the System Development Lifecycle are tracked within the POA&M data. All POA&M findings marked to be closed will be reviewed by DTI staff for the purpose of verifying sufficient evidence for closure.

9.1.9.1. Corrective Action Plan (CAP) (I/A)

A Corrective Action Plan (CAP) will identify activities planned or completed to correct deficiencies identified during the Security Assessments review. Both the POA&M and the CAP together address the remediation of security vulnerabilities and the implementation plan for security controls to reduce or eliminate known vulnerabilities in FCPS systems.

9.1.10. Privacy Impact Assessment (PIA)

The Privacy Impact Assessment (PIA) assists in identifying and addressing information privacy, information collection, and records retention & disposition when planning, developing, implementing, and operating systems that maintain information about individuals, including members of the public. The approved PIA is referenced in the Security Categorization document.

9.1.10.1. Privacy Threshold Analysis (PTA) (I/A)

A Privacy Threshold Analysis (PTA) is used to determine the privacy aspects necessary for consideration in new technology projects/programs. Some systems will not require a PIA if the system will not collect, maintain, or disseminate information about individuals. If a PIA is not required, the system should have a PTA on file documenting this determination.

9.1.11. Records Management (RM) Plan

A Records Management Plan documents the standardized administrative control of records to safeguard their existence from creation, to use, and during final disposition. The RM Plan must be consistent with the guidance required by the Maryland State Archives and Maryland Department of General Services.

9.1.12. Security Assessment Plan (SAP)

The Security Assessment Plan (SAP) addresses the purpose, scope, roles, responsibilities, management commitment, coordination among FCPS entities, and compliance as they pertain risk assessment activities for the information security boundary. The SAP must also describe how the ISO intends to implement the security requirements associated to this NIST control family.

9.1.12.1. Risk Assessment Report (RAR) (I/A)

The RAR identifies concerns that were documented during the SAP Reviewer's analysis of the security boundary and ATO Decision Package. The RAR typically provides recommendations for addressing the concerns within a specific timeframe.

9.1.13. Security Awareness and Training Plan

All FCPS information system users 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.

Individual information systems security training activities, including basic security awareness training and specific information systems security training must be documented and monitored. Individual training records are retained for 5 years (current year, plus 4 past years).

Contractors are included in FCPS's security training process, especially those who have access to FCPS Confidential information.

The Security Awareness and Training Plan provides the method for the delivery of training, content of training materials, the method of tracking/retraining completion records, and the consequences for non-completion.

9.1.14. System Architecture Documentation (SAD)

The SAD provides a comprehensive architectural overview of the system using a number of design views to depict various aspects of the system. The intent is to capture and convey the high-level design and significant architectural decisions made to the system. It will also reflect detailed updates upon the approval of future enhancements.

9.1.14.1. Information Security Architecture Documentation

The Information Security Architecture describes the overall philosophy, requirements, and approach to be taken regarding to protecting the confidentiality, integrity, and availability of system information. It describes how the information security architecture is integrated into and supports the enterprise architecture. It also contains a recording of any information security assumptions about, and dependencies on, external services.

9.1.14.2. Network Diagrams

The security boundary requires a detailed network diagram that illustrates the network topology of the system and the major components of the system, the internal and external data connections/interfaces of system components (including a description of the data flow amongst components).

9.1.15. System Inventory

A complete, current inventory of all hardware and software components within your system's authorization boundary (broken out by subsystem) must be maintained and verified annually.

9.1.15.1. Hardware Inventory

For each component, the host name, IP address (if static), role/purpose (network device, security appliances, database server, application server, web server, etc.), vendor, model number, environment (pre-production, production, etc.), physical or virtual (if virtual, the virtual host software version must be provided), and system security boundary must be supplied.

9.1.15.2. Software Inventory (Tied to each Operating System Instance)

For each component, the operating system (version), web browser (version), web application (product name, version), database (product name, version, vendor, number of databases on each host), any special applications (e.g., SharePoint, Project, FileNet, WebSphere, Adobe products, Java, custom apps), and the software's function or purpose must be supplied.

9.1.15.3. Information Inventory (PII & Confidential)

The information systems used to collect, store, and access PII & FCPS Confidential information must be listed in the *Information System Security Inventory of PII & FCPS Confidential Data*. All FCPS records containing PII must be listed in the *Inventory of Records Containing PII & FCPS Confidential Data*.

9.1.16. Security Categorization (SecCat)

The system Security Categorization defines the boundaries for the system and identifies the information that is processed on the system resulting in a determination of the overall sensitivity of the system. This document determines the level of IT security controls that are required for the system.

9.1.17. System Security Plan (SSP)

The System Security Plan (SSP) specifies, from the ISO and ISSM's perspective, the implementation of IT security controls to meet both the functional security requirements and the assurance security requirements. The current state of all controls that are required to be implemented must be documented in the SSP, the controls must address the current environment with enough detail to permit testing, and the SSP must have been updated within the last quarter prior to the assessment start date.

9.1.18. System-Specific Policies and Procedures (I/A)

Offices should develop system-specific procedures that align with FCPS operations and NIST SP 800-53 requirements. System-specific procedures support the implementation of FCPS system-specific operational requirements and associated security controls by providing step-by-step processes for performing specific functions.

9.1.18.1. Media Protection Procedures

The purpose of Media Protection Procedures ensure proper precautions are in place to protect confidential information stored on media. FCPS must restrict access to system media containing confidential information to authorized individuals. All media must be protected, especially when it 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).

9.1.18.2. Physical and Environmental Protection Procedure

The Physical and Environmental Protection Procedure contains the minimum requirements for an information security boundary's 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.

9.1.18.3. System and Information Integrity Procedure

The System and Information Integrity Procedure explains the expected implementation of 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.

The System and Information Integrity Procedure describes the system security boundary's protections against malicious code (e. g. viruses, worms, Trojan horses, etc.), intrusion detection/prevention tools, techniques and additional security protection mechanisms.

9.1.18.4. Access Control Procedure

The Access Control Procedure defines the logical access controls to the system-based mechanisms. The logical controls are 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.

9.1.18.5. Audit and Accountability Control Procedure

The Audit and Accountability Control Procedure documents the security boundary's approach to the collection, maintenance, and retention of audit trails, which record system activity by system/application processes and by user activity/processes. This procedure also documents

the audit requirements, such as the routine review by the ISO, ISSM, FCPS DTI, and auditors for inappropriate or illegal activity. The Audit and Accountability Control Procedure also contains the requirement for 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.

9.1.18.6. Identification and Authorization Procedure

Identification and Authentication Procedure defines the technical measure that prevents unauthorized users (or unauthorized processes) from entering an IT system. This procedure defines how the system is able to identify and differentiate users.

9.1.18.7. System and Communication Protection Procedure

The System and Communications Protection Procedure describes the technical mechanisms that an information security boundary 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.

10 FCPS System Security Plan (SSP) Requirements

The ATO Package requires that each security boundary ISO develop and maintain an up-to-date SSP. Appendix A of this document provides a template for documenting current cyber security measures in place and service as a template as required by MD DoIT and FCPS DTI.

10.1. Acceptable Use Enforcement

Data leakage incidents such as disclosure of non-public information or making inappropriate public statements about or for FCPS, or using FCPS resources for personal reasons, and harassing or inappropriate behavior toward another employee or student can be grounds for reprimand or dismissal. Any employee found to have violated *FCPS Regulation 300-45 Responsible Use of Digital Technology – Staff*, may be subject to disciplinary action, up to and including termination of employment. Deliberate, unauthorized disclosure of nonpublic information may result in civil and/or criminal penalties. Failure to comply with any provisions of the FCPS Security Manual may result in administrative or adverse action. Any individual with access to FCPS 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.

FCPS Security 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.

10.2. Risk Acceptance Procedures

The FCPS DTI provides IT services to FCPS Departments in support of day-to-day operations, program initiatives and overall missions. Enterprise-level IT infrastructure requires rigorous proactive administration, maintenance and upkeep to stay relevant and defend against evolving cyber threats. As such, departments that receive IT services from DTI (such as network or hosted infrastructure) inherit the operational, management, and technical benefits associated with the FCPS security program, thereby partially alleviating the department's administrative burden. The ISO should leverage the FCPS DTI documentation where applicable for the security boundary.

As a part of DTI's robust security practice, DTI 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 Departments 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.

10.2.1.1. Deviation/Waiver Acceptance Process

FCPS acknowledges that risk acceptance conditions may differ based on the circumstances presented by the security boundary seeking a risk waiver. FCPS DTI supports a Deviation/Waiver Acceptance Process for the following risk-based conditions:

10.2.1.1.1. Non-Compliance of Security Controls

Security boundary ISOs are required to document and track all control weaknesses through the Plan of Action and Milestones (POA&M) process for all systems that cannot meet the security control requirements designated within this manual and supplemental DISA STIGs. For additional information regarding POA&M requirements, see control Section 12.5.1.2 CA-5: Plan of Action and Milestones.

However, if the ISO is unable to meet the control requirements due to organizational constraints (ex. lack of funding, resources, etc.) for a period that exceeds (1) year, FCPS DTI will grant a Deviation/Waiver Acceptance for the security boundary under the following conditions:

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

When all conditions are met, FCPS DTI may issue a Deviation/Waiver Acceptance to the ISO for a defined period in which FCPS DTI will accept the risk(s) associated with the non-compliance. Additionally, the ISO will provide progress updates to FCPS DTI every 1 to 6 months depending on the severity of risk associate with non-compliance, until the issue has been fully remediated.

Vendors receiving Deviation/Waiver Acceptance will be required to provide progress updates to the contracting department on a monthly/bi-annual frequency depending on the severity of non-compliant security control(s).

Failure to meet the requirements of the POA&M, including remediation activities and reporting requirements, will result in the revocation of the security boundary's ATO and cessation of system services via network restriction and the issuance of a DATO.

10.2.1.1.2. Unsupported Software

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

As a part of the Deviation/Waiver Acceptance Process, any security boundary using unsupported software must have the approval documentation signed by the FCPS Authorizing Official (AO).

On a bi-annual cycle, the ISO will identify and validate the use of unsupported software across the local and hosted environments of the security boundary. Upon validation, the ISO will perform one of the following actions:

1. Initial/new detections of unsupported software will require that the affected ISO complete a new Deviation/Waiver Acceptance, if the deficiency cannot be rectified within 30 days;
2. Continual detections of unsupported software will require the affected ISO re-sign the existing Deviation/Waiver Acceptance;
3. Close existing Deviation/Waivers where unsupported software has been decommissioned.

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

10.3. Vendor Risk Assessment

The Frederick County Public Schools Department of Technology Infrastructure requires FCPS Information Systems and vendors that store, process, or transmit FCPS data to adhere to certain security related standards.

Adherence to the standards outlined in this document provides assurance that, at a minimum, the FCPS security boundary and vendor organizations have implemented the appropriate security controls associated with the following five (5) Trusted Service Principles:

1. Security: Systems are protected both logically and physically against unauthorized access.
2. 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).
3. 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.

4. 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.
5. Privacy: The responsible organization collects, manages, and reports on FCPS-owned sensitive data in a manner that is consistent with the privacy principles defined by the appropriate governing entity, Maryland privacy laws, and federal privacy laws.

10.3.1.1. Purpose

FCPS is committed to ensuring that all systems and vendor organizations that store, process, or transmit FCPS-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.

10.3.1.2. Conditions

FCPS and vendor organizations must provide evidence that they are compliant with the classification process provided in 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 FCPS-owned data on their hosted information system
- The vendor organization's information system interconnects with a FCPS information system
- The vendor organization's information system contains references, pointers and metadata associated to actual FCPS-owned data
- The vendor organization is developing an application that stores, processes and/or transmits sensitive state data within a FCPS-hosted environment (Partial requirements) – processing integrity and privacy principles for administrative controls

10.3.1.3. Vendor Required Security Controls

All vendors receiving, processing, storing, or accessing FCPS information are required to have the service contract routed via the FCPS contract approval process. The vendor contracts must include the following statement prior to beginning the approval process:

"Under no circumstances may any vendor/contractor/provider/consultant release, disclose, sell or otherwise use names, addresses, or any other information related to students, or staff, of

FCPS and may only use information for the purposes required under any contract/agreement or memorandum of understanding. (Refer to Maryland Student Data Privacy Act of 2015 H.B. 298, FCPS Regulation 400-20 Student Records, Board Policy 442 Student Data Privacy and FCPS Regulation 400-96 Student Data Privacy.)"

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 FCPS DTI guidelines:

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 FCPS DTI.

Auditing and Accountability – The organization must implement a logging solution to capture all activity that occurs within the environment. The organization must implement logging according to the NIST SP 800-53 Auditing and Accountability Control family, to include events such as the following at a minimum:

- 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 vendor must provide a list of individuals with access to audit logs upon request.

Data Access – all FCPS data resident on a vendor system must be made available to FCPS for local retention.

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 FCPS DTI guidelines:

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 must be compliant with NIST SP 800-52 Rev. 2 or greater based cipher methods.

Data Restrictions – The organization is restricted from transmitting and/or using FCPS production-level data within a development environment. The organization must notify FCPS 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 FCPS's approved baselines.

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

10.3.1.4. Procedures

A vendor organization that stores, processes or transmits FCPS data must provide a Risk Assessment Report (RAR) to the ISO and ISSM, 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:

- Contain 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 FCPS an acceptable level of 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 ISO and ISSM 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, FCPS 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 FCPS systems. The specific request criteria for partial RAR/SOC-2 reports will be made by the FCPS DTI on a case-by-case basis and communicated from the Awarding Department 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 Department and the FCPS DTI, 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 Department and FCPS DTI.

10.3.1.5. Production-Hosted Contract Requirements

For service organizations that host production systems/applications containing confidential data (PII, PHI, FTI) within their environment, the FCPS and the State of Maryland 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 2 Type II compliant

For organizations that do not meet either requirement, FCPS 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, FCPS 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 FCPS DTI may accept a security evaluation demonstrating an acceptable level of risk, in lieu of the requirements identified above.

11 ATO Package Submission Requirements

In order to receive an ATO Memo from the AO, a complete ATO Package, containing all required documents in Table II – ATO Package Checklist, must be submitted to the FCPS AO.

11.1.ATO Package Submission Procedure

The completed ATO Package should be uploaded to onedrive.fcps.org and shared with the FCPS AO, ISSM, ISO for the security boundary. The submitting ISO must also send an official email notification of submission.

11.2.Expert Assistance

DTI staff members are able to assist in addressing questions and providing feedback to ISOs on their ATO Package. ISO's should submit a ticket with the DTI in order to facilitate requests.

12 Appendix A: Information System Security Plan (SSP) Template

This template contains instructions, forms, and placeholder text to help produce an SO SSP. Instructions are typically in italics. Placeholder text is designated with brackets and blue highlighter (e.g., <sample placeholder>). All placeholders must be removed prior to SSP submission. To aid in formatting, Word Styles have been defined and used throughout this template. Prior to submission, remove pages 1 to 5 of this guidance document, so this page becomes page 1 of the SSP.

Information System Security Plan (SSP) for <insert System Name>

<insert date of SSP >

Revision History

Version Number	Date	Author	Description
1.0	<insert date>	<insert name>	<insert change summary>

12.1. Information System Security Plan (SSP) Overview

This SSP contains the following sections describing cyber security measures taken by the Information System Owner (ISO) for the protection of FCPS information technology systems and data:

All sections are required unless exempted by FCPS DTI and a statement explaining conditions for being exempt from compliance is provided.

12.2. General Information

1. System Name (ACRONYM)

Provide the full System name and acronym

2. Information System Owner (ISO) Name and Contact Information:

Insert the name of the ISO who is responsible for the Information Technology (IT) systems related information submitted with the SSP.

Name _____
Title _____
Telephone Number _____
Email address _____

3. Information System Security Officer (ISSO) Name and Contact Information:

Insert the name of the individual who is the ISO's point of contact for security-related matters. This individual is responsible for ensuring the accuracy of the security-related information submitted with the SSP.

Name _____
Title _____
Telephone Number _____
Email address _____

4. Executive Sponsor Name and Contact Information

Provide the name, title and contact information of the information system's Executive Sponsor

Name _____
Title _____
Telephone Number _____
Email address _____

5. Plan Date

Provide the date the plan was approved by the Executive Sponsor

_____

12.3. Maryland Information Security Manual and Frederick County Public Schools Department of Technology Infrastructure Compliance

12.3.1. Objective

The objective of security planning is to improve the protection of FCPS information system resources. The protection of a system must be documented in an System Security Plan (SSP). The development of the SSP Template is to ensure each security boundary has a standard method for documenting its compliance with the FCPS Information Security standards.

12.3.2. Purpose

The purpose of the SSP is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The SSP also delineates responsibilities and expected behavior of all individuals who access the system. The SSP should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It reflects input from various managers with responsibilities concerning the system, including information owners, the system owner, and the senior DTI information security staff.

12.3.3. SSP Requirement

FCPS requires each ISO under its jurisdiction develop and submit an SSP that address security procedures included in the FCPS WISP (Regulation Number 200-32 Data Security).

12.3.4. SSP Responsibilities

- **Director of Technology Infrastructure** – The Director of Technology Infrastructure is the FCPS Authorizing Official (AO) responsible for developing and maintaining an organization-wide information security program and provides final approval for an FCPS system's ATO memo.
- **Information System Security Manager (ISSM) -** The Information System Security Manager (ISSM) is the official responsible for serving as the Director of Technology Infrastructure's primary liaison to the ISO and ISSO.
- **Information System Owner (ISO)**– The Information System Owner (ISO) is the official responsible for the overall procurement, development, integration, modification, or operation & maintenance of the information system.
- **Information System Security Officer (ISSO) -** The Information System Security Officer (ISSO) is the official assigned responsibility by the ISO for ensuring that the appropriate operational security posture is maintained for an information system or program.

- **Authorizing Official (AO) -** The AO is a senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to FCPS operations, FCPS assets, or individuals.
- **Executive Sponsor –** The Executive Sponsor (ES) is a cabinet level official with a vested interest in the information security boundary and sub-systems contained therein. The ES is ultimately responsible for ensuring the security boundary receives and ATO and maintains an ATO throughout its lifecycle. The ES does this by formally naming the ISO for the security boundary, advocating & prioritizing appropriate department resources to maintain the ATO, and holding the ISO accountable for meeting the requirements of the ATO.

12.4. System Information

12.4.1. Security Boundary

Describe the Information System Security Boundary governed by this SSP.

- <insert text here>

12.4.2. General System Description/Purpose

Describe the organizational requirements fulfilled by the system and information processes:

- <insert text here>

12.4.3. Information System Security Categorization (SecCat):

In accordance with the determination criteria documented in Section 7 of the FCPS Information System Security Manual, insert the SecCat determination of the indicated Information System Boundary.

Choose an item.

12.4.4. Information System Operational Status:

Indicate the operational status of the identified system.

Choose an item.

12.4.5. System Environment

Provide a general description of the technical system; including a brief of the primary hardware, software, and communications equipment (Detailed Artifact: Section 9.1.14 of the FCPS Information System Security Manual).

- <insert text here>

12.4.6. Interconnection Security Agreements (ISA):

List interconnected systems, which are not directly accountable under the FCPS security management umbrella. Provide the external system name, organization name, point of contact name/title/phone/email, indicate the existence of an MOU/A (provide separately), date of agreement, purpose of interconnection. (Detailed Artifact: Section 9.1.8 of the FCPS Information Security Manual)

External System Name	
Organization Name	
Point of Contact (POC) Name	
POC Title	
POC Phone Number	
POC Email Address	
MOU/A Status	Choose an item.
MOU/A Date	Click or tap to enter a date.
Purpose of Interconnection	

12.5. Security Controls Compliance Matrix

This section of the FCPS Security Manual list of the minimum required operational security requirements for any FCPS Information System. Based on the risk evaluation, additional controls may be required. Where direct guidance is not provided, the ISO should implement the appropriate controls prescribed by the system's SecCat determination and NIST SP 800-53 Rev 4.

Valid responses within the status field:

- Yes – the requirements of the control have been satisfied
- No – the requirements of the control are not satisfied
- N/A – the control does not apply to the IS security boundary.

12.5.1. Management Level Controls

12.5.1.1. Risk Management

Security Control ID	Risk Assessment Controls	SSecCat Baseline			Status
RA-1	The ISO must develop and implement a Security Assessment Plan (SAP) that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among FCPS entities, and compliance as they pertain security & risk assessment activities for the information security boundary. The SAP must also describe how the ISO intends to implement the security requirements associated to this NIST control family. The SAP must be complimentary to the FCPS DTI SAP and be approved by the FCPS Authorizing Official. **The SAP must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**	L	M	H	
Security Categorization					
RA-2	The ISO must ensure that: a. Information and the information system are categorized in accordance with the FCPS Information System Security Manual, 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 designated representative. d. The security categorization is subject to review and revision by the FCPS Director of Technology Infrastructure.	L	M	H	
Risk Assessment					
RA-3	ISO will ensure that:	L	M	H	

	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 Information Owners, ISOs, AOs and the ISSM. 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, the ISO 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. i. Including up-to-date *FCSP Data Collection Inventory* & *FCPS Data Sharing Disclosure* 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.				
Vulnerability Scanning					
RA-5	The ISO must ensure that: a. Scans for vulnerabilities in information systems and hosted applications are conducted at least quarterly and when recommended by the ISSM, 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	L	M	H	

	automate parts of the vulnerability management process by using standards for: a. Ensuring platforms, software flaws, and improper configurations. b. Formatting, checklists and test procedures. c. Measuring vulnerability impact. c. Vulnerability scan reports and results from security control assessments are analyzed. d. Vulnerabilities are prioritized and remediated based on threat intelligence, compensating controls, and other factors, to ensure that vulnerabilities are addressed in appropriate timeframes: a. 90 days for low systems/low risk vulnerabilities b. 60 days for moderate systems/low risk, low systems/moderate risk c. 30 days for high systems/low risk, moderate systems/moderate risk, low systems/high risk d. 15 days for high systems/moderate and high risk, moderate systems/high risk, and for all critical vulnerabilities, regardless of system classification e. Timeframes could also be modified as appropriate based on the impact level of the system, vulnerability, compensating controls and likelihood of exploits. f. 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 repository for tracking and managing purpose. g. Information obtained from the vulnerability scanning process and security control assessments is shared with Information Owners, ISOs and the ISSM to help eliminate similar vulnerabilities in other information systems (e.g., systemic weaknesses or deficiencies).				
Vulnerability Scanning | Update Tool Capability					
RA-5.1	FCPS will employ vulnerability scanning tools that include the capability to readily update the information system vulnerabilities scanned.	N/A	M	H	
Vulnerability Scanning | Update by Frequency/Prior to New Scan/When Identified					

RA-5.2	FCPS will update and review vulnerability definitions and signatures prior to each scan or when new vulnerabilities are identified or reported.	N/A	M	H	
Vulnerability Scanning | Discoverable Information					
RA-5.4	FCPS will attempt to discern what information about information systems is discoverable by adversaries.	N/A	M	H	
Vulnerability Scanning | Privileged Access					
RA-5.5	FCPS will 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 activities.	N/A	M	H	

12.5.1.2. Security Assessment and Authorization

Security Control ID	Security Assessment and Authorization Controls	SSecCat Baseline			Status
CA-1	The ISO must develop and implement a Security Assessment Plan (SAP) that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among FCPS entities, and compliance as they pertain security & risk assessment activities for the information security boundary. The SAP must also describe how the ISO intends to implement the security requirements associated to this NIST control family. The SAP must be complimentary to the FCPS DTI SAP and be approved by the FCPS Authorizing Official. **The SAP plan must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**	L	M	H	
Security Assessments					
CA-2	The ISO must ensure that for each information system: a. A Security Assessment Plan (SAP) is developed that describes the scope of the assessment including: i. Security controls and control enhancements under assessment ii. Procedures to be used to determine security control effectiveness iii. Assessment environment, assessment team, and assessment roles and responsibilities b. FCPS requires that one-third of the controls be assessed annually to determine the extent to	L	M	H	

	which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The RAR compilation of the assessments is presented to the AO as part of the ATO Package to reauthorize the system. c. An RAR is produced that documents the results of the assessment d. The results of the security control assessment activities are provided, in writing, to the system ISSM or ISSM designated representative. To satisfy the requirement, ISOs 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.				
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 the FCPS Director or Technology Infrastructure. Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of organizational information systems. Independent assessments can be obtained from the FCPS DTI or can be contracted to public or private sector entities outside of organizations. The DTI Information Security Team is managed in such a manner as to create impartiality in the evaluation of FCPS information systems. The Authorizing Official 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	M	H	
Security Assessments | Specialized Assessment					
CA-2.2	Annual, announced penetration testing must be included as a part of security control assessments.	N/A	N/A	H	

	This enhancement only applies to High categorization systems. If any High systems are introduced in the future, these requirements will be further defined.				
System Interconnections					
CA-3	The ISO 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. (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.	N/A	M	H	
System Interconnections | Restriction on External System Configuration					
CA-3.5	The FCPS IS must employ a **deny-all**, **allow-by exception** policy for allowing FCPS environments and systems to connect to external information systems.	N/A	M	H	
Plan of Action and Milestones					
CA-5	The ISO 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.	L	M	H	

	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.				
Security Authorization					
CA-6	The FCPS has assigned the Director of Technology Infrastructure to the role of AO for information systems. The AO must: a. Ensure the authorizing official authorizes information systems for processing before commencing operations. b. Update the security authorization on an annual basis or upon significant change to the system that may require reauthorization.	L	M	H	
Continuous Monitoring					
CA-7	The ISO 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 FCPS 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 FCPS officials (AO, ISSM) annually. A subset of security controls (1/3) is assessed annually during continuous monitoring and reauthorization efforts.	L	M	H	

	The FCPS ISSM, collaborating with the Director of Technology Infrastructure, establishes the selection criteria and subsequent subset for assessment.				
Continuous Monitoring | Independent Assessment					
CA-7.1	FCPS 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 Director of Technology Infrastructure. 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. The AO determines 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	M	H	
Penetration Testing					
CA-8	FCPS must conduct penetration testing on an annual basis on information systems containing sensitive PII.	N/A	M	H	
Penetration Testing | Independent Penetration Testing Agent or Team					
CA-8.1	Employ an independent penetration testing agent or team to perform penetration testing on the system or system components. Independent penetration testing agents or teams are individuals or groups who conduct impartial penetration testing of organizational systems. Impartiality implies that penetration testing agents or teams are free from perceived or actual conflicts of interest with respect to the development, operation, or management of the systems that are the targets of the penetration testing. The DTI Information Security Team is managed in such a manner as to create impartiality in the evaluation of FCPS information systems. CA-2(1) provides additional information on independent assessments that can be applied to penetration testing.	N/A	M	H	
Penetration Testing | Red Team Exercises					
CA-8.2	Employ the following red-team exercises to simulate attempts by adversaries to compromise organizational	N/A	N/A	H	

	systems in accordance with applicable rules of engagement: Red team exercises extend the objectives of penetration testing by examining the security and privacy posture of organizations and the capability to implement effective cyber defenses. Red team exercises simulate attempts by adversaries to compromise mission and business functions and provide a comprehensive assessment of the security and privacy posture of systems and organizations. Such attempts may include technology-based attacks and social engineering-based attacks. Technology-based attacks include interactions with hardware, software, or firmware components and/or mission and business processes. Social engineering-based attacks include interactions via email, telephone, shoulder surfing, or personal conversations. Red team exercises are most effective when conducted by penetration testing agents and teams with knowledge of and experience with current adversarial tactics, techniques, procedures, and tools. While penetration testing may be primarily laboratory-based testing, organizations can use red team exercises to provide more comprehensive assessments that reflect real-world conditions. The results from red team exercises can be used by organizations to improve security and privacy awareness and training and to assess control effectiveness.				
Penetration Testing | Facility Penetration Testing					
CA-8.3	Employ a penetration testing process that includes alternating annual announced/unannounced attempts to bypass or circumvent controls associated with physical access points to the facility. Penetration testing of physical access points can provide information on critical vulnerabilities in the operating environments of organizational systems. Such information can be used to correct weaknesses or deficiencies in physical controls that are necessary to protect organizational systems.	N/A	M	H	
Internal System Connections					
CA-9	The ISO must ensure that: a. Information systems' internal connections are authorized.	L	M	H	

	b. For each internal connection, the interface characteristics, security requirements, and the nature of the information communicated are documented.				

12.5.1.3. Planning

Security Control ID	Security Planning Controls	SSecCat Baseline			Status
PL-1	The ISO must develop and implement a Security Assessment Plan (SAP) that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance as they pertain to security & risk assessment activities within the organization and describes how ISO intends to implement the security requirements associated with this NIST control family. The SAP must be complimentary to the FCPS DTI SAP and be approved by the FCPS Authorizing Official. **The SAP must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**	L	M	H	
	System Security Plan				
PL-2	The ISO must ensure that: a. A security plan is developed for the information system security boundary that: 1. Is consistent with the FCPS's enterprise architecture 2. Explicitly defines the security boundary for the system 3. Describes the operational context of the information system, within the security boundary, 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	L	M	H	

	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 ISO, ISSM, 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 FCPS officials (e.g. ISO, ISSM, 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. e. The security plan is protected from unauthorized disclosure and modification.				
System Security Plan | Coordinate with Other Organizational Entities					
PL-2.3	The ISO 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 FCPS DTI Cybersecurity personnel, ISOs, technical leads/system administrators, etc. before conducting such activities in order to reduce the impact on other organizational entities.	N/A	M	H	
Rules of Behavior					
PL-4	FCPS must ensure that: a. All personnel read the Acceptable Use Policy, which outlines expected behavior and responsibilities about information and information systems usage. b. The Acceptable Use Policy is readily available to all FCPS employees and individuals requiring access to the information system including personnel with administrative privileges to ensure they handle the elevated privileges properly. c. Signed acknowledgements are received from users indicating that they have read, understand, and agree to abide by the Acceptable Use Policy before	L	M	H	

	authorizing access to information and information system. d. The Acceptable Use Policy is reviewed and updated on an annual basis. e. 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.				
Rules of Behavior | Social Media and Networking Restrictions					
PL-4.1	FCPS 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	M	H	
Concept of Operations					
PL-7	The CONOPS may be included in the security or privacy plans for the system or in other system development life cycle documents. The CONOPS is a living document that requires updating throughout the system development life cycle. For example, during system design reviews, the concept of operations is checked to ensure that it remains consistent with the design for controls, the system architecture, and the operational procedures. Changes to the CONOPS are reflected in ongoing updates to the security and privacy plans, security and privacy architectures, and other organizational documents, such as procurement specifications, system development life cycle documents, and systems engineering documents. a. Develop a Concept of Operations (CONOPS) for the system describing how the organization intends to operate the system from the perspective of information security and privacy; and b. Review and update the CONOPS annually. Related to: PL-2, SA-2, SI-12	L	M	H	
Information Security Architecture					
PL-8	The ISO must: a. Develop, as part of the SAD, 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.	L	M	H	

	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.				
Central Management					
PL-9	Central management refers to organization-wide management and implementation of selected controls and processes. This includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed controls and processes. As the central management of controls is generally associated with the concept of common (inherited) controls, such management promotes and facilitates standardization of control implementations and management and the judicious use of organizational resources. Centrally managed controls and processes may also meet independence requirements for assessments in support of initial and ongoing authorizations to operate and as part of organizational continuous monitoring. Automated tools (e.g., security information and event management tools or enterprise security monitoring and management tools) can improve the accuracy, consistency, and availability of information associated with centrally managed controls and processes. Automation can also provide data aggregation and data correlation capabilities; alerting mechanisms; and dashboards to support risk-based decision-making within the organization. As part of the control selection processes, organizations determine the controls that may be suitable for central management based on resources and capabilities. It is not always possible to centrally manage every aspect of a control. In such cases, the control can be treated as a hybrid control with the control managed and implemented centrally or at the system level. The controls and control	L	M	H	

	enhancements that are candidates for full or partial central management include but are not limited to: AC-2(1), AC-2(2), AC-2(3), AC-2(4), AC-4(all), AC-17(1), AC-17(2), AC-17(3), AC-17(9), AC-18(1), AC-18(3), AC-18(4), AC-18(5), AC-19(4), AC-22, AC-23, AT-2(1), AT-2(2), AT-3(1), AT-3(2), AT-3(3), AT-4, AU-3, AU-6(1), AU-6(3), AU-6(5), AU-6(6), AU-6(9), AU-7(1), AU-7(2), AU-11, AU-13, AU-16, CA-2(1), CA-2(2), CA-2(3), CA-3(1), CA-3(2), CA-3(3), CA-7(1), CA-9, CM-2(2), CM-3(1), CM-3(4), CM-4, CM-6, CM-6(1), CM-7(2), CM-7(4), CM-7(5), CM-8(all), CM-9(1), CM-10, CM-11, CP-7(all), CP-8(all), SC-43, SI-2, SI-3, SI-4(all), SI-7, SI-8.				

12.5.1.4. Program Management

Security Control ID	Program Management	SSecCat Baseline			Status
	Information Security Program Plan				
PM-1	a. Develop and disseminate an organization-wide information security program plan that: 1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; 2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 3. Reflects the coordination among organizational entities responsible for information security; and 4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; b. Review and update the organization-wide information security program plan [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and	L	M	H	

	c. Protect the information security program plan from unauthorized disclosure and modification.				
Information Security Program Leadership Role					
PM-2	Appoint a senior agency information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.	L	M	H	
Information Security and Privacy Resources					
PM-3	a. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement; b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards; and c. Make available for expenditure, the planned information security and privacy resources.	N/A	M	H	
Plan of Action and Milestones Process					
PM-4	a. Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems: 1. Are developed and maintained; 2. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and 3. Are reported in accordance with established reporting requirements. b. Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	L	M	H	
System Inventory					
PM-5	Develop and update annually an inventory of organizational systems.	L	M	H	

System Inventory | Inventory of Personally Identifiable Information					
PM-5.1	Establish, maintain, and update annually an inventory of all systems, applications, and projects that process personally identifiable information.	L	M	H	
Measures of Performance					
PM-6	Develop, monitor, and report on the results of information security and privacy measures of performance.	L	M	H	
Enterprise Architecture					
PM-7	Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.	L	M	H	
Critical Infrastructure Plan					
PM-8	Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.	L	M	H	
Risk Management Strategy					
PM-9	a. Develops a comprehensive strategy to manage: 1. Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; and 2. Privacy risk to individuals resulting from the authorized processing of personally identifiable information; b. Implement the risk management strategy consistently across the organization; and c. Review and update the risk management strategy annually or as required, to address organizational changes.	L	M	H	
Authorization Process					
PM-10	a. Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes; b. Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and c. Integrate the authorization processes into an organization-wide risk management program.	L	M	H	
Mission and Business Process Definition					
PM-11	a. Define organizational mission and business processes with consideration for information security and privacy and	L	M	H	

	the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determine information protection and personally identifiable information processing needs arising from the defined mission and business processes; and c. Review and revise the mission and business processes annually.				
Insider Threat Program					
PM-12	Implement an insider threat program that includes a cross-discipline insider threat incident handling team.	L	M	H	
Security and Privacy Workforce					
PM-13	Establish a security and privacy workforce development and improvement program.	L	M	H	
Testing, Training, and Monitoring					
PM-14	a. Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems: 1. Are developed and maintained; and 2. Continue to be executed; and b. Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	L	M	H	
Security and Privacy Groups and Associations					
PM-15	Establish and institutionalize contact with selected groups and associations within the security and privacy communities: a. To facilitate ongoing security and privacy education and training for organizational personnel; b. To maintain currency with recommended security and privacy practices, techniques, and technologies; and c. To share current security and privacy information, including threats, vulnerabilities, and incidents.	L	M	H	
Threat Awareness Program					
PM-16	Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.	L	M	H	

Protecting Controlled Unclassified Information on External Systems					
PM-17	a. Establish policy and procedures to ensure that requirements for the protection of controlled unclassified information that is processed, stored or transmitted on external systems, are implemented in accordance with applicable laws, executive orders, directives, policies, regulations, and standards; and b. Review and update the policy and procedures annually.	L	M	H	
Privacy Program Plan					
PM-18	a. Develop and disseminate an organization-wide privacy program plan that provides an overview of the agency's privacy program, and: 1. Includes a description of the structure of the privacy program and the resources dedicated to the privacy program; 2. Provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements; 3. Includes the role of the senior agency official for privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities; 4. Describes management commitment, compliance, and the strategic goals and objectives of the privacy program; 5. Reflects coordination among organizational entities responsible for the different aspects of privacy; and 6. Is approved by a senior official with responsibility and accountability for the privacy risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; and b. Update the plan annually and to address changes in federal privacy laws and policy and organizational changes and problems identified during plan implementation or privacy control assessments.	L	M	H	
Privacy Program Leadership Role					
PM-19	Appoint a senior agency official for privacy with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the organization-wide privacy program.	L	M	H	

Dissemination of Privacy Program Information					
PM-20	Maintain a central resource webpage on the organization's principal public website that serves as a central source of information about the organization's privacy program and that: a. Ensures that the public has access to information about organizational privacy activities and can communicate with its senior agency official for privacy; b. Ensures that organizational privacy practices and reports are publicly available; and c. Employs publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.	L	M	H	
Accounting of Disclosures					
PM-21	a. Develop and maintain an accurate accounting of disclosures of personally identifiable information, including: 1. Date, nature, and purpose of each disclosure; and 2. Name and address, or other contact information of the individual or organization to which the disclosure was made; b. Retain the accounting of disclosures for the length of the time the personally identifiable information is maintained or five years after the disclosure is made, whichever is longer; and c. Make the accounting of disclosures available to the individual to whom the personally identifiable information relates upon request.	L	M	H	
Personally Identifiable Information Quality Management					
PM-22	Develop and document organization-wide policies and procedures for: a. Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle; b. Correcting or deleting inaccurate or outdated personally identifiable information; c. Disseminating notice of corrected or deleted personally identifiable information to individuals or other appropriate entities; and d. Appeals of adverse decisions on correction or deletion requests.	L	M	H	

Data Governance Body					
PM-23	Establish a Data Governance Body consisting of [Assignment: organization-defined roles] with [Assignment: organization-defined responsibilities].	L	M	H	
Data Integrity Board					
PM-24	Establish a Data Integrity Board to: a. Review proposals to conduct or participate in a matching program; and b. Conduct an annual review of all matching programs in which the agency has participated.	L	M	H	
Minimization of PII Used in Testing, Training, and Research					
PM-25	a. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research; b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes; c. Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; and d. Review and update policies and procedures annually.	L	M	H	
Complaint Management					
PM-26	Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and privacy practices that includes: a. Mechanisms that are easy to use and readily accessible by the public; b. All information necessary for successfully filing complaints; c. Tracking mechanisms to ensure all complaints received are reviewed and addressed within ten business days; d. Acknowledgement of receipt of complaints, concerns, or questions from individuals within ten business days; and e. Response to complaints, concerns, or questions from individuals within ten business days.	L	M	H	
Privacy Reporting					
PM-27	a. Develop [Assignment: organization-defined privacy reports] and disseminate to:	L	M	H	

	1. [Assignment: organization-defined oversight bodies] to demonstrate accountability with statutory, regulatory, and policy privacy mandates; and 2. [Assignment: organization-defined officials] and other personnel with responsibility for monitoring privacy program compliance; and b. Review and update privacy reports quarterly.				
Risk Framing					
PM-28	a. Identify and document: 1. Assumptions affecting risk assessments, risk responses, and risk monitoring; 2. Constraints affecting risk assessments, risk responses, and risk monitoring; 3. Priorities and trade-offs considered by the organization for managing risk; and 4. Organizational risk tolerance; b. Distribute the results of risk framing activities to [Assignment: organization-defined personnel]; and c. Review and update risk framing considerations annually.	L	M	H	
Risk Management Program Leadership Roles					
PM-29	a. Appoint a Senior Accountable Official for Risk Management to align organizational information security and privacy management processes with strategic, operational, and budgetary planning processes; and b. Establish a Risk Executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across the organization.	L	M	H	
Supply Chain Risk Management Strategy					
PM-30	a. Develop an organization-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services;	L	M	H	

	1. Implement the supply chain risk management strategy consistently across the organization; and a). Review and update the supply chain risk management strategy on an annual basis or as required, to address organizational changes.				
Continuous Monitoring Strategy					
PM-31	Develop an organization-wide continuous monitoring strategy and implement continuous monitoring programs that include: a. Establishing the following organization-wide metrics to be monitored: [Assignment: organization-defined metrics]; b. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness; c. Ongoing monitoring of organizationally-defined metrics in accordance with the continuous monitoring strategy; d. Correlation and analysis of information generated by control assessments and monitoring; e. Response actions to address results of the analysis of control assessment and monitoring information; and f. Reporting the security and privacy status of organizational systems to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].	L	M	H	
Purposing					
PM-32	Analyze [Assignment: organization-defined systems or systems components] supporting mission essential services or functions to ensure that the information resources are being used consistent with their intended purpose.	L	M	H	

12.5.2. Operational Level Controls

12.5.2.1. Awareness and Training

Security Control ID	Security Awareness and Training Controls	SSecCat Baseline	Status

AT-1	The ISO must develop and implement a Security Awareness and Training Plan that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance as they pertain to security & risk assessment activities within the organization and describes how ISO intends to implement the security requirements associated with this NIST control family. The Security Awareness and Training Plan must be complimentary to the FCPS DTI guidance and be approved by the FCPS Authorizing Official. **The Security and Awareness Plan must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**	L	M	H	
Security Awareness Training					
AT-2	All FCPS information system users 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.	L	M	H	
Security Awareness Training | Insider Threat					
AT-2.2	The ISO 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. The Security Awareness and Training Plan should include a plan for insider threat monitoring and an insider threat training implementation, in the vent indicators of an insider threat are recognized.	N/A	M	H	

Role-Based Security Training					
AT-3	The ISO 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 FCPS Confidential information 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 FCPS and the information systems to which personnel have authorized access.	L	M	H	
Security Training Records					
AT-4	FCPS 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 FCPS Confidential information.	L	M	H	
Vulnerability Scanning | Update by Frequency/Prior to New Scan/When Identified					
PL-8	The ISO must: d. Develop, as part of the SAD, 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. e. Review and update the information security architecture at least annually to reflect updates in the enterprise architecture.	L	M	H	

	f. Ensure that planned information security architecture changes are reflected in the security plan, the security Concept of Operations, and organizational procurements/acquisitions.				

12.5.2.2. Configuration Management

Security Control ID	Configuration Management Controls	SSecCat Baseline			Status
CM-1	The ISO must develop and implement a Configuration Management Plan (CMP) that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance as they pertain to security & risk assessment activities within the organization and describes how ISO intends to implement the security requirements associated with this NIST control family. The CMP must be complimentary to the FCPS DTI guidance and be approved by the FCPS Authorizing Official. **The CMP must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**	L	M	H	
Baseline Configuration					
CM-2	Baseline documentation must exist for all systems within a security boundary. The ISO must ensure that current baseline configurations of information system components are developed, documented, and maintained under configuration control. NOTE: For FCPS (non-COTS) applications, the System Baseline Configuration, within the CMP, should document the following; • Versions 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	L	M	H	

	• All Known security assumptions, implications, system level protections, best practices, and required permissions
	• Deployment configuration settings
	  o Encryption settings (data in transit)
	  o PKI Certificate Configuration Settings
	  o Password Settings				

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	M	H	
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	H	
Baseline Configuration | Retention of Previous Configurations					
CM-2.3	At a minimum, a single iteration of the previous 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.	N/A	N/A	H	
Baseline Configuration | Configure Systems, Components, or Devices for High Risk Area					
CM-2.7	Access to the FCPS network resources and systems from foreign countries is currently prohibited. No information systems or system components may be used during foreign travel to perform FCPS related work. a. Where an exception to this policy is needed, then approval must be obtained from Department Senior management through a request submitted to the Director of Technology Infrastructure well in advance.	L	M	H	

	b. The Department must ensure the following if approval is to be provided: a. No personally owned mobile devices will be used on foreign travel to perform government related work. b. Only FCPS approved and furnished mobile devices are allowed. c. Approved foreign travel devices including any removable media must be configured to encrypt stored data using FIPS 140-2 validated encryption. d. Device must provide protection against malware. e. Travelers must ensure physical security of the device while in transit and while on foreign travel or foreign duty. c. Loss, theft or compromise of assigned mobile devices while on travel should be immediately reported to the DTI Incident Response Team (IRT).				
Configuration Change Control					
CM-3	The ISO 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 documented in the Security Impact Analysis (SIA). c. Configuration- change decisions associated with the information system are documented in the Change Control Log. d. Approved configuration-controlled changes to the information system are implemented, with implementation verification recorded in the Change Control Log. 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	N/A	M	H	

	Change Control Board (CCB) that must convene weekly to review upcoming configuration changes.				
Configuration Change Control | Automated Document/Notification 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 CCB 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	H	
Configuration Change Control | Test/Validate/Document Changes					
CM-3.2	Changes to information systems must be tested, validated, and documented Change Control Log before being implemented on the operational system.	N/A	M	H	
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.	L	M	H	
Security Impact Analysis | Separate Test Environment					
CM-4.1	Changes to critical information systems providing essential services to FCPS and constituents, must be analyzed in a separate test environment before installation in an operational environment. This analysis must look for security and operational impacts due to flaws, weaknesses, incompatibility, or intentional malice.	L	M	H	
Access Restrictions for Change					
CM-5	Physical and logical access restrictions associated with changes to information systems must be defined, documented, approved, and enforced. ISO must ensure a formal approval process is in place for granting individuals the authority to perform system changes.	N/A	M	H	
Access Restrictions for Change | Automated Access Enforcement/Auditing					

CM-5.1	FCPS 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	H	
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 and Change Control Log must be periodically reviewed, at least semiannually. 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	H	
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 FCPS DTI. 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	H	
Configuration Settings					
CM-6	The ISO 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. a. FCPS information systems are required to meet the configuration settings established in Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGs), complemented by 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,	L	M	H	

	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 System Baseline Configuration. Deviations must be documented and recorded in the AO-Approved Deviation and Waiver Log. d. Changes to configuration settings are monitored and controlled.				
Configuration Settings | Automated Central Management/Application/Verification					
CM-6.1	The ISO 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	H	
Configuration Settings | Respond to Unauthorized Change					
CM-6.2	The ISO 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	H	
Least Functionality					
CM-7	FCPS 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 DISA STIGs and CIS Benchmarks.	L	M	H	
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, M-Cast, Bluetooth, etc.	N/A	M	H	
Least Functionality | Prevent Program Execution					
CM-7.2	FCPS must ensure that the information systems prohibit unauthorized or unapproved software from executing on information system components according to approved software list and CCB approval.	N/A	M	H	
Least Functionality | Unauthorized Software/Blacklisting					

CM-7.4	The ISO must ensure that: a. Software programs that are explicitly not authorized to execute on the information system are identified and documented. FCPS DTI employs a whitelist that identifies all software authorized to execute on the information system. All software not listed on the whitelist is deemed as prohibited. 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 technologies require explicit approval from FCPS DTI and 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. FCPS also establishes restrictions on the use of open source software. Open source software must: a) Be legally licensed b) Approved by the FCPS DTI c) Adhere to a secure configuration baseline checklist from the US Government or industry.	N/A	M	H	
Least Functionality | Authorized Software/Whitelisting					
CM-7.5	The ISO 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.	N/A	M	H	
Information System Component Inventory					
CM-8	An inventory of information system components must be: a. developed, documented, and maintained and must:	L	M	H	

	1. Accurately reflect the current information system. 2. Include all components within the authorization boundary of the information system that store, process or transmit FCPS Confidential 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: i. Point of Contact or Owner ii. Inventory tag or Serial Number iii. Operating System (OS) Vendor Name iv. Operating System (OS) Version Number v. Operating System (OS) Patch Level vi. Fully Qualified Domain Name (FQDN) vii. IP Address/Hostname (if static) viii. Make and Model (when applicable) ix. Physical Location 2. Inventory requirements for system software for servers, workstations, and laptops of various kinds and uses in production and pre-production environments: i. Point of Contact ii. Software Vendor Name iii. Software Version Number Reviews and updates of the information system component inventory should be done at least annually or when information system changes occur.				
Information Systems Component Inventory | Updates During Installation/Removal					
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	M	H	
Information Systems 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.	N/A	N/A	H	

	This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.				
Information Systems Component Inventory | Automated Unauthorized Component Detection					
CM-8.3	The ISO 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 FCPS officials (ISO, ISSM etc.) are notified when deviations or unauthorized software is discovered.	N/A	M	H	
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	H	
Information System Component Inventory | No Duplicate Account of Components					
CM-8.5	The ISO must ensure that all components within the security 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	M	H	
Configuration Management Plan (CMP)					
CM-9	The ISO 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, establishing a Change Control Board (CCB), b. Establishes process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items.	N/A	M	H	

	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.				
Software Usage Restrictions					
CM-10	The ISO must ensure that: a. Software and associated documentation are 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 open source software is controlled and documented to address the software is legally licensed, approved by the FCPS DTI and adheres to secure configuration baseline checklist(s) provided by the US Government.	L	M	H	
User Installed Software					
CM-11	FCPS must ensure that: a. User software installation is prohibited and procedural enforcement methods governing the installation of software by users are established. b. Software installation procedures 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.	L	M	H	

12.5.2.3. Contingency Planning

Security Control ID	Contingency Planning Controls	SSecCat Baseline			Status
CP-1	The ISO must develop and implement a Contingency Plan / Disaster Recovery Plan (CP/DRP) that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance as they pertain to security & risk assessment activities within the organization and describes how ISO intends to implement the security requirements associated with this NIST control family.	L	M	H	

	The CP/DRP must be complimentary to the FCPS DTI guidance and be approved by the FCPS Authorizing Official. **The CP/DRP must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**				
Contingency Plan					
CP-2	The ISO must ensure that: a. Contingency plans are developed for information systems and security boundaries 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 the FCPS 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 FCPS, 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.	L	M	H	

	g. The contingency plan is protected from unauthorized disclosure and modification.				
Contingency Plan | Coordinate with Related Plans					
CP-2.1	The ISO must ensure that CP/DRP development is coordinated with organizations responsible for related plans (e.g., Incident Response Plan).	N/A	M	H	
Contingency Plan | Capacity Planning					
CP-2.2	FCPS 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	H	
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 CP/DRP after activation of the CP/DRP.	N/A	M	H	
Contingency Plan | Resume All Mission/Business Functions					
CP-2.4	FCPS must ensure that the resumption of all missions and business functions within the time frame specified in the system CP/DRP 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	H	
Contingency Plan | Continue Essential Missions/Business Functions					
CP-2.5	The ISO 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	H	
Contingency Plan | Identify Critical Assets					
CP-2.8	FCPS must identify all critical information system assets supporting essential missions and business functions.	N/A	M	H	
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	L	M	H	

	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.				
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	H	
Contingency Plan Testing					
CP-4	The ISO must ensure that: a. Contingency plans for the information system are tested and/or exercised at least annually using tests defined within the approved Contingency Test Plan. b. Contingency plan test/exercise are documented within the Contingency Test Plan and results are recorded within the Contingency Test Report. c. Corrective actions are initiated as needed and recorded within the POA&M.	L	M	H	
Contingency Plan Testing | Coordinate with Related Plans					
CP-4.1	Contingency plan testing and/or exercises must be coordinated with FCPS organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations	N/A	N/A	H	

	Plan, Business Recovery Plan, and Incident Response Plan, Emergency Action Plan).				
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	H	
Alternate Storage Site					
CP-6	FCPS 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	M	H	
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. The FCPS Director of Technology Infrastructure 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	M	H	
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	H	
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 within the CP/DRP.	N/A	M	H	
Alternate Processing Site					

CP-7	FCPS 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 documented within the AO approved CP/DRP, based on the business continuity requirements (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	M	H	
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. FCPS 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	M	H	
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 SSP or CP/DRP.	N/A	M	H	
Alternate Processing Site | Priority of Service					
CP-7.3	FCPS must ensure that alternate processing site agreements contain priority of service provisions in accordance with the BIA, SSP, and CP/DRP availability	N/A	M	H	

	requirements including recovery time objectives are developed.				
Alternate Processing Site | Preparation for Use					
CP-7.4	The ISO 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	H	
Telecommunication Services					
CP-8	The ISO 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	M	H	
Telecommunications Services | Priority of Service Provision					
CP-8.1	The ISO must ensure that: a. Primary and alternate telecommunication service agreements are developed that contain priority-of-service provisions in accordance with FCPS'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	M	H	
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	M	H	
Telecommunications Services | Separation of Primary/Alternate Providers					
CP-8.3	FCPS must ensure that alternate telecommunications services are obtained from providers that are separated	N/A	N/A	H	

	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.				
Telecommunications Services | Provider Contingency Plan					
CP-8.4	The ISO 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 FCPS 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	H	
Information System Backup					
CP-9	The ISO must ensure that: a. Full 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.	L	M	H	
Information System Backup | Testing for Reliability/Integrity					
CP-9.1	Back-up information must be tested, in accordance with the Contingency Test Plan, at least annually to verify media reliability and information integrity. The test results must be recorded within the Contingency Test Report.	N/A	M	H	
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.	N/A	M	H	

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	H	
Information System Backup | Transfer to Alternate Storage Site					
CP-9.5	The ISO 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 for cloud facilities 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.	L	M	H	
Information System Recovery and Reconstitution					
CP-10	The ISO must provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. For FCPS applications, testing should occur at least annually in accordance with the Contingency Test Plan, and results recorded in the Contingency Test Report to verify security remains in place when an application failure occurs.	L	M	H	
Information System Recovery and Reconstitution | Transaction Recovery					
CP-10.2	The ISO must implement transaction recovery for FCPS transaction-based information systems.	N/A	M	H	
Information System Recovery and Reconstitution | Restore Within Time Period					
CP-10.4	The ISO must ensure the capability to restore information system components within the time frame defined in the system CP/DRP, from configuration-controlled and	N/A	N/A	H	

	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.				

12.5.2.4. Incident Response

Security Control ID	Incident Response Controls	SSecCat Baseline			Status
IR-1	The ISO must develop and implement an Incident Response Plan (IRP) that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance as they pertain to security & risk assessment activities within the organization and describes how ISO intends to implement the security requirements associated with this NIST control family. The IRP must be complimentary to the FCPS DTI guidance and be approved by the FCPS Authorizing Official. **The IRP must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**	L	M	H	
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	L	M	H	
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	H	
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	H	
Incident Response Testing					
IR-3	The ISO must ensure the incident response capability for the information system security boundary is tested and/or exercised at least annually using tests and/or exercises defined by the ISSM or outlined in the Contingency Test Plan and test results are documented in the Contingency Test Report. FCPS 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 within a security boundary.	L	M	H	
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	M	H	
Incident Handling					
IR-4	The ISO must ensure that:	L	M	H	

	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.				
Incident Handling | Automated Incident Handling Process					
IR-4.1	The ISO must employ automated mechanisms to support the incident handling process.	N/A	M	H	
Incident Handling | Information Correlation					
IR-4.4	FCPS must correlate incident information and individual incident responses to achieve an organization- wide perspective on incident awareness and response.	N/A	M	H	
Incident Monitoring					
IR-5	FCPS must ensure information system security incidents are tracked and documented on an ongoing basis.	L	M	H	
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.	L	M	H	
Incident Reporting					
IR-6	The ISO must: a. Require personnel to report a suspected or verified security incident to the DTI incident response team (DTI IRT) immediately upon discovery. b. Ensure that security incident information is reported to the DTI IRT as applicable. The security boundary IRT 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, security boundary IRT 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 DTI IRT, who will report to USCERT, if required.	L	M	H	

	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				
Incident Response Assistance					
IR-7	The ISO 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.	L	M	H	
Incident Response Assistance | Automated Support for Availability of Information/Support					
IR-7.1	FCPS must employ automated mechanisms to increase the availability of incident response-related information and support.	N/A	M	H	
Incident Response Plan					
IR-8	The ISO must ensure that: a. An Incident Response Plan (IRP) is developed that: 1. Provides the roadmap for implementing the 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 FCPS Incident Response Plan. 4. Meets the unique FCPS and Department 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.	L	M	H	

	8. Is reviewed and approved by the designated AO. b. Copies of the incident response plan are distributed to ISOs, ISSM, AO, and other key personnel as deemed necessary. c. The IRP is reviewed annually. d. The IRP 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 ISOs, ISSM, AO, etc. f. Incident response plan is protected from unauthorized disclosure and modification.				
Information Spillage Response					
IR-9	The ISO should examine the information spillage procedures and determine if the procedures detail the FCPS 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 DTI 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.	L	M	H	

12.5.2.5. Maintenance

Security Control ID	Maintenance Controls	SSecCat Baseline			Status
MA-1	The ISO must develop and implement a Configuration Management Plan (CMP), which contains a Maintenance Plan (MA) that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance as they pertain to security & risk assessment activities within the organization and describes how ISO intends to implement	L	M	H	

	the security requirements associated with this NIST control family. The MA must be complimentary to the FCPS DTI guidance and be approved by the FCPS Authorizing Official. **The MA must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**				
Controlled Maintenance					
MA-2	The ISO must ensure that: a. Scheduling, performance, documentation, and review of maintenance and repairs on information system components is conducted in accordance with manufacturer or vendor specifications and/or FCPS DTI 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 ISO explicitly approves the removal of information systems or information system components from FCPS facilities for off-site maintenance or repairs as applicable, excluding Hard Disk Drives (HDD) of any kind. FCPS does not allow the HDD to be removed from FCPS Facilities to non-FCPS Facilities for any reason. d. Functioning equipment is sanitized to remove all information from associated media prior to removal from FCPS facilities for off-site maintenance or repairs; Hard disk drives (HDD) are excluded and not permitted to be sent to non-FCPS facilities. 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 Log.	L	M	H	
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	H	
Maintenance Tools					
MA-3	FCPS approves, controls, and monitors information system maintenance tools. The maintenance methodology, tools, and activities are documented and approved within the Maintenance Plan.	N/A	M	H	
Maintenance Tools | Inspect Tools					
MA-3.1	All maintenance tools (e.g., diagnostic and test equipment) carried into FCPS facilities by maintenance personnel must be inspected for improper and unauthorized modifications.	N/A	M	H	
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	M	H	
Maintenance Tools | Prevent Unauthorized Removal					
MA-3.3	The ISO must prevent the unauthorized removal of maintenance equipment containing organizational information by: a. Verifying that there is no FCPS 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	H	
Non-Local Maintenance					
MA-4	The ISO must ensure that: a. Third Parties and unvetted personnel complete approved non-local maintenance and diagnostics activities through chaperoned access, using an	L	M	H	

	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 DTI guidelines and as documented in Maintenance Plan 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, in the Maintenance Log for non-local maintenance and diagnostic activities and recorded when possible using screen recording software. e. All sessions and network connections are terminated when non-local maintenance is completed.				
Non-Local Maintenance | Document Non-Local Maintenance					
MA-4.2	The plan and guidelines for the establishment and use of non-local maintenance and diagnostic connections should be documented in information system Maintenance Plan.	N/A	M	H	
Non-Local Maintenance | Comparable Security/Sanitization					
MA-4.3	The ISO 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 FCPS information) prior to non-local maintenance or diagnostic services and before removal from FCPS 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	H	
Maintenance Personnel					
MA-5	The ISO must ensure that:	L	M	H	

	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 qualified and 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.				
Maintenance Personnel | Individuals Without Appropriate Access					
MA-5.1	The ISO 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.	N/A	N/A	H	

	This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.				
Timely Maintenance					
MA-6	The ISO must ensure that maintenance support and/or spare parts for information system security-critical components are obtained within 48 hours or less of failure or as otherwise defined in maintenance agreements and the system CP/DRP or standard operating procedures. Security-critical components may include, for example, firewalls, guards, gateways, intrusion detection systems, audit repositories, authentication servers, and intrusion prevention systems.	N/A	M	H	

12.5.2.6. Media Protection

Security Control ID	Media Protection Controls	SSecCat Baseline			Status
MP-1	The ISO must develop and implement a Media Protection Procedure, meeting the minimum standards established in the FCPS DTI Media Protection Procedures, that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance as they pertain to security & risk assessment activities within the organization and describes how ISO intends to implement the security requirements associated with this NIST control family. The Media Protection Procedure must be complimentary to the FCPS DTI guidance and be approved by the FCPS Authorizing Official. **The Media Protection Procedure must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**	L	M	H	
Media Access					
MP-2	The ISO 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.	L	M	H	

Media Marking					
MP-3	The ISO 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	M	H	
Media Storage					
MP-4	The ISO must ensure that: a. All digital and non-digital information system media are physically controlled and securely stored within FCPS 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	M	H	
Media Transport					
MP-5	The ISO must ensure that: a. Both digital and nondigital media are protected and controlled during transport outside of controlled area using FCPS defined security safeguards, defined in the Media Protection Procedures. 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 FCPS 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.	L	M	H	
Media Transport | Cryptographic Protection					
MP-5.4	The ISO 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	N/A	M	H	

	information stored on digital media during transport outside of controlled areas.				
Media Sanitization					
MP-6	The ISO must: a. Sanitize information system media, both digital and non-digital, prior to disposal, release from FCPS 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, FCPS 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.	L	M	H	
Media Sanitization | Review/Approve/Track/Document/Verify					
MP-6.1	Media sanitization and disposal actions must be approved, tracked, documented, and verified in accordance with the security boundary's Records Management Plan.	L	M	H	
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.	L	M	H	
Media Sanitization | Nondestructive Techniques					
MP-6.3	Portable, removable storage devices must be sanitized, in accordance with the approved Media Protection Procedures, upon issuance and reissuance prior to connecting such devices to information systems.	L	M	H	
Media Use					
MP-7	The ISO 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 FCPS approved portable storage devices that are FIPS 140-2 certified should be used.	L	M	H	
Media Use | Prohibit Use Without Owner					

MP-7.1	The OSP must prohibit the use of portable storage devices in organizational information systems when such devices have no identifiable owner.	N/A	M	H	

12.5.2.7. Physical and Environmental Security

Security Control ID	Physical and Environmental Protection Controls	SSecCat Baseline			Status
PE-1	The ISO must develop and implement a Physical and Environmental Protection Procedure, meeting the minimum standards established in the FCPS DTI Physical and Environmental Protection Procedures, that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance as they pertain to security & risk assessment activities within the organization and describes how ISO intends to implement the security requirements associated with this NIST control family. The Physical and Environmental Protection Procedure must be complimentary to the FCPS DTI guidance and be approved by the FCPS Authorizing Official. **The Physical and Environmental Protection Procedure must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**	L	M	H	
Physical Access Authorizations					
PE-2	The ISO 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. FCPS enforces physical access authorizations to the information system in addition to the physical access	L	M	H	

	controls, where Confidential information is received, processed, stored, or transmitted.				
Physical Access Control					
PE-3	The ISO 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: o Verifying individual access authorization before granting access to the facility. b. For environments containing systems categorized as Moderate and above: • Physical access audit logs (digital or physical) 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 FCPS defined safeguards (security cameras). • Visitors are escorted, and visitor activities are monitored when maintenance is performed on FCPS devices by outside vendors that do not have FCPS 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.	L	M	H	
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).	N/A	N/A	H	

	This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.				
Access Control for Transmission Medium					
PE-4	The ISO must ensure that access to all information system distribution and transmission lines within facilities hosting FCPS 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	M	H	
Access Control for Output Devices					
PE-5	The ISO 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	M	H	
Monitoring Physical Access					
PE-6	The ISO 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 FCPS DTI IRT.	L	M	H	
Monitoring Physical Access | Intrusion Alarms/Surveillance Equipment					
PE-6.1	The ISO must monitor physical intrusion alarms and surveillance equipment.	N/A	M	H	
Monitoring Physical Access | Monitoring Physical Access to Information Systems					
PE-6.4	The ISO must monitor physical access to the information system in addition to the physical access monitoring of the FCPS DTI-defined physical spaces containing one or more components of the high risk information system.	N/A	M	H	
Visitor Access Records					
PE-8	The ISO must ensure, for facilities that are protected by FCPS, 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:	L	M	H	

	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. Purpose of visit 6. Name and organization of person visited b. Visitor access records are reviewed at least monthly.				
Visitor Access Records | Automated Records Maintenance/Review					
PE-8.1	The ISO 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	H	
Power Equipment and Cabling					
PE-9	The ISO must ensure power equipment and power cabling for information systems are protected from damage and destruction.	N/A	M	H	
Emergency Shutoff					
PE-10	The ISO 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	M	H	
Emergency Power					
PE-11	The ISO must ensure the 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	M	H	
Emergency Power | Long-Term Alternate Power Supply – Minimal Operational Capability					
PE-11.1	The ISO 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	M	H	
Emergency Lighting					
PE-12	The ISO 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.	L	M	H	

Fire Protection					
PE-13	The ISO must employ and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source.	L	M	H	
Fire Protection | Detection Devices/Systems					
PE-13.1	The ISO 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	H	
Fire Protection | Suppression Devices/Systems					
PE-13.2	Fire suppression devices/systems should provide automatic notification of any activation to designated FCPS 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	H	
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	M	H	
Temperature and Humidity Controls					
PE-14	FCPS must ensure that: a. Temperature and humidity levels within facilities containing information systems are maintained between 62- and 80-degrees Fahrenheit and humidity levels maintained between 5% to 45% year-round. b. Temperature and humidity controls are monitored regularly.	L	M	H	
Water Damage Protection					
PE-15	FCPS must ensure the 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.	L	M	H	
Water Damage Protection | Automated 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 FCPS 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	H	
Delivery and Removal					

PE-16	The ISO 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.	L	M	H	
Alternate Work Site					
PE-17	The ISO 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	M	H	
Location of Information System Components					
PE-18	FCPS 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. 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	H	

12.5.2.8. Personnel Security

Security Control ID	Personnel Security	SSecCat Baseline			Status
PS-1	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] personnel security policy that: a). Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b). Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;	L	M	H	

	b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personnel security policy and procedures; and c. Review and update the current personnel security: 1. Policy annually and following [Assignment: organization-defined events]; and 2. Procedures annually and following [Assignment: organization-defined events].				
Position Risk Designation					
PS-2	a. Assign a risk designation to all organizational positions; b. Establish screening criteria for individuals filling those positions; and c. Review and update position risk designations annually.	L	M	H	
Personnel Screening					
PS-3	a. Screen individuals prior to authorizing access to the system; and b. Rescreen individuals in accordance with [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of rescreening].	L	M	H	
Personnel Termination					
PS-4	Upon termination of individual employment: a. Disable system access within 24 hours; b. Terminate or revoke any authenticators and credentials associated with the individual; c. Conduct exit interviews that include a discussion of [Assignment: organization-defined information security topics]; d. Retrieve all security-related organizational system-related property; and e. Retain access to organizational information and systems formerly controlled by terminated individual.	L	M	H	
Personnel Termination | Post-Employment Requirements					
PS-4.1	a. Notify terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information; and b. Require terminated individuals to sign an acknowledgment of post-employment requirements as part of the organizational termination process.	L	M	H	
Personnel Termination | Automated Actions					
PS-4.2	Use [Assignment: organization-defined automated mechanisms] to [Selection (one or more): notify [Assignment: organization-defined personnel or roles] of individual termination actions; disable access to system resources].	L	M	H	

Personnel Transfer					
PS-5	a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization; b. Initiate [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action]; c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and d. Notify [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].	L	M	H	
Access Agreements					
PS-6	a. Develop and document access agreements for organizational systems; b. Review and update the access agreements annually; and c. Verify that individuals requiring access to organizational information and systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or annually.	L	M	H	
Access Agreements | Classified Information Requiring Special Protection					
PS-6.2	Verify that access to classified information requiring special protection is granted only to individuals who: a. Have a valid access authorization that is demonstrated by assigned official government duties; b. Satisfy associated personnel security criteria; and c. Have read, understood, and signed a nondisclosure agreement.	L	M	H	
Access Agreements | Post-Employment Requirements					
PS-6.3	a. Notify individuals of applicable, legally binding post-employment requirements for protection of organizational information; and b. Require individuals to sign an acknowledgment of these requirements, if applicable, as part of granting initial access to covered information.	L	M	H	

External Personnel Security					
PS-7	a. Establish personnel security requirements, including security roles and responsibilities for external providers; b. Require external providers to comply with personnel security policies and procedures established by the organization; c. Document personnel security requirements; d. Require external providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within [Assignment: organization-defined time period]; and e. Monitor provider compliance with personnel security requirements.	L	M	H	
Personnel Sanctions					
PS-8	a. Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures; and b. Notify [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.	L	M	H	
Position Descriptions					
PS-9	Incorporate security and privacy roles and responsibilities into organizational position descriptions.	L	M	H	

12.5.2.9. Supply Chain Risk Management

Security Control ID	Supply Chain Risk Management	SSecCat Baseline			Status
Policy and Procedures					
SR-1	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] supply chain risk management policy that:	L	M	H	

	a). Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b). Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and c. Review and update the current supply chain risk management: 1. Policy at least annually and following to address threat, organizational or environmental changes; and 2. Procedures at least annually and following to address threat, organizational or environmental changes.				
Supply Chain Risk Management Plan					
SR-2	a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: [Assignment: organization-defined systems, system components, or system services]; b. Review and update the supply chain risk management plan at least annually or as required, to address threat, organizational or environmental changes; and c. Protect the supply chain risk management plan from unauthorized disclosure and modification.	L	M	H	
Supply Chain Risk Management Plan | Establish SCRM Team					
SR-2.1	Establish a supply chain risk management team consisting of [Assignment: organization-defined personnel, roles, and responsibilities] to lead and support the following SCRM activities: [Assignment: organization-defined supply chain risk management activities].	L	M	H	

Supply Chain Controls and Processes					
SR-3	a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [Assignment: organization-defined system or system component] in coordination with [Assignment: organization-defined supply chain personnel]; b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events: [Assignment: organization-defined supply chain controls]; and c. Document the selected and implemented supply chain processes and controls in [Selection: security and privacy plans; supply chain risk management plan; [Assignment: organization-defined document].	L	M	H	
Supply Chain Controls and Processes | Diverse Supply Base					
SR-3.1	Employ a diverse set of sources for the following system components and services: [Assignment: organization-defined system components and services].	L	M	H	
Supply Chain Controls and Processes | Limitation of Harm					
SR-3.2	Employ the following controls to limit harm from potential adversaries identifying and targeting the organizational supply chain: [Assignment: organization-defined controls].	L	M	H	
Supply Chain Controls and Processes | Sub-Tier Flow Down					
SR-3.3	Ensure that the controls included in the contracts of prime contractors are also included in the contracts of subcontractors.	L	M	H	
Provenance					
SR-4	Document, monitor, and maintain valid provenance of the following systems, system components, and associated data: [Assignment: organization-defined systems, system components, and associated data].	L	M	H	
Acquisition Strategies, Tools, and Methods					
SR-5	Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [Assignment: organization-defined acquisition strategies, contract tools, and procurement methods].	L	M	H	
Supplier Assessments and Review					
SR-6	Assess and review the supply chain-related risks associated with suppliers or contractors and the system,	L	M	H	

	system component, or system service they provide annually.				
Supplier Assessments and Reviews | Testing and Analysis					
SR-6.1	Employ [Selection (one or more): organizational analysis; independent third-party analysis; organizational testing; independent third-party testing] of the following supply chain elements, processes, and actors associated with the system, system component, or system service: [Assignment: organization-defined supply chain elements, processes, and actors].	L	M	H	
Supply Chain Operations Security					
SR-7	Employ the following Operations Security (OPSEC) controls to protect supply chain-related information for the system, system component, or system service: [Assignment: organization-defined Operations Security (OPSEC) controls].	L	M	H	
Notification Agreements					
SR-8	Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the [Selection (one or more): notification of supply chain compromises; results of assessments or audits; [Assignment: organization-defined information]].	L	M	H	
Tamper Resistance and Detection					
SR-9	Implement a tamper protection program for the system, system component, or system service.	N/A	N/A	H	
Tamper Resistance and Detection | Multiple Stages of SDLC					
SR-9.1	Employ anti-tamper technologies, tools, and techniques throughout the system development life cycle.	N/A	N/A	H	
Inspection of Systems or Components					
SR-10	Inspect the following systems or system components [Selection (one or more): at random; at [Assignment: organization-defined frequency], upon [Assignment: organization-defined indications of need for inspection]] to detect tampering: [Assignment: organization-defined systems or system components].	L	M	H	
Component Authenticity					
SR-11	a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and b. Report counterfeit system components to [Selection (one or more): source of counterfeit component; [Assignment: organization-defined external reporting	L	M	H	

	organizations]; [Assignment: organization-defined personnel or roles]].				
Component Authenticity | Anti-Counterfeit Training					
SR-11.1	Train [Assignment: organization-defined personnel or roles] to detect counterfeit system components (including hardware, software, and firmware).	L	M	H	
Component Authenticity | Configuration Control for Component Service and Repair					
SR-11.2	Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service: [Assignment: organization-defined system components].	L	M	H	
Component Authenticity | Anti-Counterfeit Scanning					
SR-11.3	Scan for counterfeit system components quarterly.	L	M	H	
Component Disposal					
SR-12	Dispose of [Assignment: organization-defined data, documentation, tools, or system components] using the following techniques and methods: [Assignment: organization-defined techniques and methods].	L	M	H	

12.5.2.10. System and Information Integrity

Security Control ID	System and Information Integrity Controls	SSecCat Baseline			Status
SI-1	The ISO must develop and implement a System and Information Integrity Procedure, meeting the minimum standards established in the FCPS DTI Procedures, that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance as they pertain to security & risk assessment activities within the organization and describes how ISO intends to implement the security requirements associated with this NIST control family. The System and Information Integrity Procedure must be complimentary to the FCPS DTI guidance and be approved by the FCPS Authorizing Official. **The System and Information Integrity Procedure must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**	L	M	H	
Flaw Remediation					

SI-2	The ISO 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 FCPS 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 and Confidential data. 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 FCPS DTI. d. Vulnerabilities identified to be at a Critical Level must be remediated within 15 days of announcement. e. Vulnerabilities identified to be at a High Level must be remediated within 30 days of announcement. f. Flaw remediation is incorporated into the configuration management processes.	L	M	H	
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	H	
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	M	H	
Malicious Code Protection					
SI-3	The ISO 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	L	M	H	

	with the security boundary's approved Configuration Management Plan 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 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.				
Malicious Code Protection | Central Management					
SI-3.1	FCPS must ensure malicious code protection mechanisms are centrally managed.	N/A	M	H	
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	M	H	
Information System Monitoring					
SI-4	The ISO 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 security boundary to collect DTI determined essential information; and (ii) at ad hoc locations within the system to track specific types of transaction of interest to DTI.	L	M	H	

	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 FCPS 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 ISSM and Director of Technology Infrastructure as needed. h. Notify Administrators by real-time alerts or e-mail notices when potentially malicious traffic is identified.				
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	M	H	
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	M	H	
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	M	H	

Security Alerts, Advisories, and Directives					
SI-5	The ISO 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 ISSM, Director of Technology Infrastructure, 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.	L	M	H	
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 FCPS 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	H	
Security Function Verification					
SI-6	The ISO should verify the correct operation of organization defined security functions; perform verification of system startup, restart, shutdown, upon command with appropriate privileges, semi-annually. When anomalies are discovered, either the system administrator must be notified, or the system must shut down or restarted.	L	M	H	
Software, Firmware, and Information Integrity					
SI-7	The ISO 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	M	H	
Software, Firmware, and Information Integrity | Integrity Checks					

SI-7.1	The ISO 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	M	H	
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	H	
Software, Firmware, and Information Integrity | Automated Response to Integrity Violations					
SI-7.5	The ISO 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	H	
Software, Firmware, and Information Integrity | Integration of Detection and Responses					
SI-7.7	The ISO 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	M	H	
Software, Firmware, and Information Integrity | Binary or Machine Executable Code					
SI-7.14	The ISO 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.	N/A	M	H	
Spam Protection					
SI-8	The ISO 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.	N/A	M	H	

	b. Spam protections are updated when new releases are available in accordance with the security boundary's Configuration Management Plan.				
Spam Protection | Central Management					
SI-8.1	Spam Protection mechanisms should be centrally managed.	N/A	M	H	
Spam Protection | Automatic Updates					
SI-8.2	The ISO should automatically update spam protection mechanisms for security boundaries.	N/A	M	H	
Information Input Validation					
SI-10	The ISO 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	M	H	
Error Handling					
SI-11	The FCPS 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, FCPS should also ensure applications are secure during startup and shutdown, as well as conduct fuzz testing prior to application releases.	N/A	M	H	
Information Handling and Retention					
SI-12	The ISO 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 the Records Management Plan, which accounts for 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.	L	M	H	
Memory Protection					
SI-16	All FCPS 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	M	H	

12.5.2.11. System and Services Acquisition

Security Control ID	System and Services Acquisition Controls	SSecCat Baseline			Status
SA-1	The ISO must review the FCPS System and Services Acquisition policies, regulations, and procedures that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance as they pertain to security & risk assessment activities within the security boundary and provide supplemental documentation describing how ISO intends to implement the security requirements associated with this NIST control family, if the existing guidance is insufficient. The SA must be complimentary to the FCPS DTI guidance and be approved by the FCPS Authorizing Official. **The SA must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**	L	M	H	
Allocation of Resources					
SA-2	The ISO must determine, document, and allocate the resources required to protect the information system and services as part of the planning processes. Resource allocations include initial system/service establishment and sustained operations & maintenance for the intended period of performance. The department should establish a discrete budget line item for the security of the acquired system or service.	L	M	H	
Acquisition Process					
SA-4	All FCPS acquisitions involving information system, system component, or information system services must include the following requirements, descriptions, and criterial, explicitly or by reference, in the acquisition contract: • Security functionality requirements (e.g. capabilities, functions and mechanisms) • Security strength requirements (e.g. correctness, completeness, resistance to direct attack, and resistance to tampering or bypass) • Security assurance requirements	L	M	H	

	○ Development processes, procedures, practices, and methodologies ○ Evidence of security functionality from development and assessment activities • Security related documentation requirements as determined by the type and sensitivity of the data being protected • Protection of security related documentation requirements • Description of the development and production environments, in which the system is intended to operate • Acceptance criteria Information system components are discrete, identifiable information technology assets (e.g., hardware, software, or firmware) that represent the building blocks of an information system. Information system components include commercial information technology products.				
Acquisition Process | Functional Properties					
SA-4.1	The developer of the information system, system component or information system service must provide a description of the functional properties of the security controls to be employed.	N/A	M	H	
Information System Documentation					
SA-5	The ISO must obtain administrator documentation for the information system, system component, or information system service that describes: • Secure configuration, installation, and operation • Effective use and maintenance of security functions/mechanisms • Known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions	N/A	M	H	
Security Engineering Principles					
SA-8	The ISO must apply information system security engineering principles in the specification, design, development, implementation, and modification of the information system. Security engineering principles include, for example:	N/A	M	H	

	• developing layered protections; • establishing sound security policy, architecture, and controls as the foundation for design; • incorporating security requirements into the system development life cycle; • delineating physical and logical security boundaries; • ensuring that system developers are trained on how to build secure software; • tailoring security controls to meet organizational and operational needs; • performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; • reducing risk to acceptable levels, thus enabling informed risk management decisions.				
External Information System Services					
SA-9	FCPS requires all external information systems service providers comply with FCPS information security requirements, and employ the appropriate security controls defined in the FCPS DTI Information System Security Manual and applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance (e.g. HIPAA, PCI DSS, etc.). The ISO must define and document, within the SAP the methods employed to monitor the security compliance of external service providers on an ongoing basis.	N/A	M	H	
External Information System Services | Identification of Functions/Ports/Protocols/Services					
SA-9.2	The ISO must require the providers of external systems or services identify the functions, ports, protocols, and other services necessary for the use of the identified services. Information from external service providers regarding the specific functions, ports, protocols, and services used in the provisioning of services can be particularly useful when the need arises to understand the risk & functional trade-offs involved in restricting certain services or blocking certain ports/protocols.	N/A	M	H	

Developer Configuration Management					
SA-10	FCPS requires the developer of an internal or external information system, system component, or information system service to: • Perform configuration management during the system, component, or service implementation and operation. • Document, manage, and control the integrity of changes to the infrastructure, operating system, software, and firmware • Implement only FCPS-approved changes • Document approved changes and their potential security impacts • Track security flaws and flaw resolutions, reporting findings to the ISO	N/A	M	H	
Developer Security Testing and Evaluation					
SA-11	The ISO Should require the developer of information system, system component, or information system service to: • Develop, document, and implement a security assessment plan • Perform appropriate testing and evaluation for the security of the system • Produce evidence of security assessment execution and results • Implement verifiable flaw remediation processes • Correct flaws identified during testing/evaluation, within expected SLAs.	N/A	M	H	
Supply Chain Protection					
SA-12	FCPS must protect against supply chain threats to the information system, system component, or information system service by employing necessary security safeguards as part of a comprehensive, defense-in-breadth strategy. The acquisition/procurement processes should require supply chain entities implement necessary security safeguards to:	N/A	N/A	H	

	• reduce the likelihood of unauthorized modifications at each stage in the supply chain; • protect information systems and information system components, prior to taking delivery of such systems/components. This control enhancement also applies to information system services. Security safeguards include, for example: • security controls for development systems, development facilities, and external connections to development systems; • vetting development personnel; and • use of tamper-evident packaging during shipping/warehousing. NOTE: This enhancement only applies to High categorization systems. If any High systems are introduced in the future, this requirement will be further defined.				
Critical Analysis					
SA-14	The ISO must identify and document in the BIA & CP/DRP critical information system components and functions by performing a criticality analysis.	L	M	H	

12.5.3. Technical Level Controls

12.5.3.1. Access Control Requirements

Security Control ID	Access Controls	SSecCat Baseline			Status
AC-1	The ISO must develop and implement an Access Control Procedure, meeting the minimum standards established in the FCPS DTI Procedures, that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance as they pertain to security & risk assessment activities within the organization and describes how ISO intends to implement the security requirements associated with this NIST control family.	L	M	H	

	The Access Control Procedure must be complimentary to the FCPS DTI guidance and be approved by the FCPS Authorizing Official. **The Access Control Procedure must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**				
Account Management					
AC-2	All FCPS information systems must manage information system accounts by: 1. Identifying account types (e.g., individual, system, application, and temporary); NOTE: Guest/Anonymous/Group 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 Manual and any associated FCPS DTI 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;	L	M	H	

	Privileged accounts are reviewed at least semiannually.				
Account Management | Automated System Management					
AC-2.1	Automated mechanisms should be employed to support the management of information system accounts.	N/A	M	H	
Account Management | Removal of Temporary/Emergency Accounts					
AC-2.2	Temporary access accounts to FCPS 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	M	H	
Account Management | Disable Inactive Accounts					
AC-2.3	Information systems must automatically disable inactive accounts after **60 days of inactivity**. FCPS 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	M	H	
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	M	H	
Account Management | Inactivity Logout					
AC-2.5	The ISO must require that user's application sessions automatically **logout after 15 minutes of inactivity** has been reached.	L	M	H	
Account Management | Usage Conditions					
AC-2.11	The ISO must ensure that the information system enforces FCPS DIT-defined circumstances and/or usage conditions for FCPS DTI-defined information system accounts. The ISO 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 ISO 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	H	
Account Management | Account Monitoring/ Atypical Use					
AC-2.12	The ISO must:	N/A	N/A	H	

	• 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 FCPS DTI 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.				
Account Management | Disable Accounts for High-Risk Individuals					
AC-2.13	The ISO 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	H	
Access Enforcement					
AC-3	The ISO must ensure that all information systems enforce assigned authorizations for logical access to the information system, that all default manufacturer usernames/passwords are changed, and that only authorized personnel are given access to the stored configuration files.	L	M	H	
Information Flow Enforcement					
AC-4	The ISO must ensure that information systems enforce approved authorizations for controlling the flow of information within the system and between interconnected systems. The appropriate tools 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, are employed to facilitate adequate flow control. 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	M	H	
Separation of Duties					

AC-5	All FCPS 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: a. System Administration or operation (assuring systems function, to serve the system users) b. System Access Management (account creation, modification, removal, etc.) c. System Security (assuring adequacy of system controls for availability, integrity, and confidentiality) d. System Management (allocating adequate resources for implementation of effective IT Security Programs and system controls)	N/A	M	H	
Least Privilege					
AC-6	FCPS 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 FCPS missions and business functions. The ISO 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	M	H	
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	M	H	
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	M	H	
Least Privilege | Network Access to Privileged Commands					
AC-6.3	The ISO 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	H	
Least Privilege | Privileged Accounts					
AC-6.5	The ISO must restrict privileged accounts on the information system to qualified system administrators. Personnel, who no longer require this level of access, should be promptly removed from the approved access list.	N/A	M	H	
Least Privilege | Auditing Use of Privileged Functions					
AC-6.9	FCPS 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	M	H	
Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions					
AC-6.10	FCPS information systems must prevent non-privileged users from executing privileged functions to include, but not limited to: • 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	M	H	
Unsuccessful Login Attempts					
AC-7	FCPS information systems access accounts must:	L	M	H	

	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/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.				
System Use Notification					
AC-8	All FCPS 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 Frederick County Public Schools 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 FCPS warning banner:	L	M	H	

	"By logging onto this device, you agree to adhere to all applicable Frederick County Public Schools (FCPS) Board of Education Policies and FCPS Regulations. **This system is for education, official, or authorized use only. FCPS systems are subject to monitoring for maintenance, to preserve system integrity and security, and for other official purposes. There is no expectation to privacy regarding information created, sent, received, used, or stored on this system. Board of Education Policy 208 Data Security, 421 Student Records, 442 Student Data Privacy, FCPS Regulation 300-45 Acceptable Use of Digital Technology – Staff, 400-73 Responsible Use of Digital Technology – Student, 200-32 Data Security, 400-18 Electronic Devices_Student Use, 400-20 Student Records, 400-96 Student Data Privacy, and all other policies and regulations as they apply to use of this system. Violation of these policies and regulations may result in disciplinary action. In addition, FCPS reserves the right to report any suspected illegal activities to the appropriate authorities."** Any deviation from this official banner should be approved by FCPS DTI.				
Concurrent Session Control					
AC-10	FCPS 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	M	H	
Session Lock					
AC-11	FCPS 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, pursuant to AC-2.5. "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	M	H	
Session Lock | Pattern Hiding Displays					
AC-11.1	FCPS information systems must conceal, via the session lock, information previously visible on the display with a publicly viewable image.	N/A	M	H	
Session Termination					

AC-12	The ISO 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, FCPS 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	M	H	
Permitted Actions Without Identification or Authentication					
AC-14	FCPS information systems must: a. Identify systems and system actions that can be performed on the information system without identification and authentication consistent with the FCPS mission/business function must be documented. Public information can be accessed without identification or authentication, when appropriately documented. 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.	L	M	H	
Remote Access					
AC-17	The ISO 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 and documented by the ISO or designee prior to allowing such connections. c. Multi-factor authentication mechanisms are employed for all remote access to the network.	L	M	H	

	d. When administrative actions are performed from external connections, the use of an encrypted VPN connection is required.				
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	M	H	
Remote Access | Protection of Confidentiality/Integrity Using Encryption					
AC-17.2	Cryptographic mechanisms must be used to protect the confidentiality and integrity of all remote access sessions.	N/A	M	H	
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	M	H	
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.	L	M	H	
Wireless Access					
AC-18	FCPS 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.	L	M	H	
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	M	H	
Wireless Access | Restrict Configuration by Users					
AC-18.4	The ISO must identify and explicitly authorize the users allowed to independently configure wireless networking capabilities. FCPS 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	H	
Wireless Access | Antennas/Transmission Power Levels					

AC-18.5	The ISO 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	H	
Access Control for Mobile Devices					
AC-19	Mobile devices used to access FCPS information systems, must be configured with at least one factor of authentication (e.g. PIN, fingerprint, facial recognition).	L	M	H	
Access Control for Mobile Devices | Full Device/Container-Based Encryption					
AC-19.5	The ISO must enforce the use of 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	M	H	
Use of External Information Systems					
AC-20	The ISO 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: a. Personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); b. Privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); c. Information systems owned or controlled by non-governmental organizations; and d. Government information systems that are not owned by, operated by, or under the direct supervision and authority of FCPS.	L	M	H	
Use of External Information Systems | Limits on Authorized Use					
AC-20.1	The ISO must ensure that only permitted authorized individuals use an external information system to access the information system or to process, store, or transmit FCPS-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.	N/A	M	H	

	b. Approved information system connection or processing agreements with the organizational entity hosting the external information system are retained. c. An approved VPN Access Form has been submitted to FCPS.				
Use of External Information Systems | Portable Storage Devices					
AC-20.2	The ISO must restrict the use and connection of portable storage devices on FCPS information systems to those with a business need, and require any storage media containing information identified as sensitive, by the data owner, 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	M	H	
Information Sharing					
AC-21	The ISO 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 Confidential 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 FCPS contracts, SLAs, ISAs, or MOUs.	N/A	M	H	
Publicly Accessible Content					
AC-22	The ISO must ensure that: a. Individuals are designated to post information onto FCPS 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 is reviewed for nonpublic information is reviewed prior to posting on FCPS information systems to ensure that nonpublic information is not included. d. The content on publicly accessible FCPS information systems is reviewed for nonpublic information prior to posting and at least quarterly; and nonpublic information is removed from publicly accessible FCPS information systems, if discovered.	L	M	H	

12.5.3.2. Audit and Accountability Control Requirements

Security Control ID	Audit and Accountability Controls	SSecCat Baseline			Status
AU-1	The ISO must develop and implement an Audit and Accountability Control Procedure, meeting the minimum standards established in the FCPS DTI Procedures, that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance as they pertain to security & risk assessment activities within the organization and describes how ISO intends to implement the security requirements associated with this NIST control family. The Audit and Accountability Control Procedure must be complimentary to the FCPS DTI guidance and be approved by the FCPS Authorizing Official. **The Audit and Accountability Control Procedure must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**	L	M	H	
Audit Events					
AU-2	The ISO 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	L	M	H	

	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 FCPS 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. 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 FCPS DTI 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 ISO must review the list of auditable events for information systems annually. The ISSM reviews and updates the minimum list of auditable events annually.	N/A	M	H	
Content of Audit Records					
AU-3	FCPS 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	L	M	H	

	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				
Content of Audit Records | Additional Audit Information					
AU-3.1	FCPS 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	M	H	
Content of Audit Records | Centralized Management of Planned Audit Record Content					
AU-3.2	FCPS 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	H	
Audit Storage Capacity					
AU-4	FCPS must ensure that sufficient audit record storage capacity is allocated for information systems to prevent log files from filling up between log rotation intervals. FCPS 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 the system, and retained for a period of **7 years**.	L	M	H	

Response to Audit Processing Failure					
AU-5	The ISO must ensure that, in the event of an audit processing failure, information systems: a. Alert designated FCPS 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) and Audit and Accountability Control Procedure. c. Provide a warning when allocated audit record storage volume reaches a maximum audit record storage capacity.	L	M	H	
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	H	
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	H	
Audit Review, Analysis, and Reporting					
AU-6	The ISO 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 and Audit and Accountability Control Procedure, for each system. b. Any findings are documented and reported to FCPS DTI designated officials including incident response team, and if necessary findings are escalated to the Director of Technology Infrastructure.	L	M	H	

	All information systems connected to a FCPS network should utilize the DTI-approved centralized audit record management solution with the requirements defined by the ISSM 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.				
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 FCPS DTI processes for investigation and response to suspicious activities.	N/A	M	H	
Audit Review, Analysis, and Reporting | Correlate Audit Repositories					
AU-6.3	The ISO must ensure that information system audit records are analyzed and correlated across different repositories to gain organization-wide situational awareness.	N/A	M	H	
Audit Review, Analysis, and Reporting | Integration/Scanning and Monitoring Capabilities					
AU-6.5	The ISO 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	H	
Audit Review, Analysis, and Reporting | Correlation with Physical Monitoring					
AU-6.6	The ISO 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	H	
Audit Reduction and Report Generation					
AU-7	FCPS 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.	N/A	M	H	

	FCPS 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 FCPS DTI enterprise audit generation tools due to system functionality and operational requirements must have documented in its system security plan (SSP) and Audit and Accountability Control Procedure, the process by which its logs may be sorted, organized, and accessed for more meaningful analysis.				
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	M	H	
Time Stamps					
AU-8	FCPS 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 deviation requirement.	L	M	H	
Time Stamps | Synchronization with Authoritative Time					
AU-8.1	FCPS information systems must: a. Compare the internal information system clocks at least daily with the FCPS NTP time source. b. Synchronize, if the offset is greater than 1 second, the internal system clocks to the FCPS NTP server. c. The FCPS NTP server must synchronize with a minimum of three authenticated NTP time sources with a stratum level of 5 or higher (1-5) that maintains synchronization with NIST.	L	M	H	
Protection of Audit Information					
AU-9	FCPS information systems must protect audit information and audit tools from unauthorized access, use, modification, and deletion.	L	M	H	
Protection of Audit Information | Audit Backup on Separate Physical System/Components					
AU-9.2	FCPS 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.	N/A	N/A	H	

	This enhancement only applies to High categorization systems. If any High systems are introduced in the future, these requirements will be further defined.				
Protection of Audit Information | Cryptographic Protection					
AU-9.3	FCPS 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	H	
Protection of Audit Information | Access by Subset of Privileged Users					
AU-9.4	The ISO 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 Audit and Accountability Procedures. FCPS 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	M	H	
Non-Repudiation					
AU-10	ISOs 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	H	
Audit Record Retention					

AU-11	FCPS 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.	L	M	H	
Audit Generation					
AU-12	FCPS 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 FCPS DTI 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.	L	M	H	
Audit Generation | System-Wide/Time-Correlated Audit Trail					
AU-12.1	Audit records, from all information system components eligible for the DTI-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	H	
Cross-Organizational Auditing					
AU-16	The ISO must capture the identity of individuals issuing requests at the initial information system, and subsequent systems record that the requests emanated from authorized individuals. FCPS 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	M	H	

12.5.3.3. Identification and Authorization Control Requirements

Security Control ID	Identification and Authorization Controls	SSecCat Baseline			Status
IA-1	The ISO must develop and implement an Identification and Authorization Control Procedure, meeting the minimum standards established in the FCPS DTI Procedures, that addresses the purpose, scope, roles,	L	M	H	

	responsibilities, management commitment, coordination among organizational entities, and compliance as they pertain to security & risk assessment activities within the organization and describes how ISO intends to implement the security requirements associated with this NIST control family. The Identification and Authorization Control Procedure must be complimentary to the FCPS DTI guidance and be approved by the FCPS Authorizing Official. **The Identification and Authorization Control Procedure must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**				
Identification and Authentication (Organizational Users)					
IA-2	All FCPS 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.	L	M	H	
Identification and Authentication | Network Access to Privileged Accounts					
IA-2.1	FCPS information systems must be capable of Single Sign-On (SSO) integration with valid FCPS DTI SSO services. FCPS Information systems should implement multifactor authentication using a FCPS DTI approved token for network access to privileged accounts. In the event an approved deviation from this control is granted, the minimum acceptable identification and authentication criteria for FCPS information systems requires the use of an individual identifier (e.g. username) and one factor of authentication (e.g. complex password). 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 ISO 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.	L	M	H	

	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. f. System or Administrator generated passwords must be required to be changed upon first logon. 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.				
Identification and Authentication | Network Access to Non-Privileged Accounts					
IA-2.2	FCPS information systems must be capable of Single Sign-On (SSO) integration with valid FCPS DTI SSO services. FCPS Information systems should implement multifactor authentication using a FCPS DTI approved token for network access to non-privileged accounts. In the event an approved deviation from this control is granted, the minimum acceptable identification and authentication criteria for FCPS information systems requires the use of an individual identifier (e.g. username) and one factor of authentication (e.g. complex password). 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 ISO 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. f. System or Administrator generated passwords must be required to be changed upon first logon. 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	M	H	
Identification and Authentication | Local Access to Privileged Accounts					

IA-2.3	FCPS information systems should implement multifactor authentication for local access to privileged accounts. The use of null passwords is prohibited. Deviation from this control, must at least meet the deviation standards documented in IA-2.1. 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	M	H	
Identification and Authentication | Local Access to Non-Privileged Accounts					
IA-2.4	FCPS 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	H	
Identification and Authentication | Network Access to Privileged Accounts – Replay Resistant					
IA-2.8	FCPS 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	M	H	
Identification and Authentication | Network Access to Non-Privileged Accounts – Replay Resistant					
IA-2.9	FCPS 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	H	

Identification and Authentication | Remote Access – Separate Device					
IA-2.11	FCPS information systems must implement systems capable of Single Sign-On (SSO) integration with valid FCPS DTI SSO services. FCPS 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. In the event an approved deviation from this control is granted, the minimum acceptable identification and authentication criteria for FCPS information systems requires the use of an individual identifier (e.g. username) and one factor of authentication (e.g. complex password).	N/A	M	H	
Identification and Authentication | Acceptance of PIV Credentials					
IA-2.12	For FCPS systems where Personal Identity Verification (PIV) or like standard credentials are issued, information systems with sensitive data must be designed to accept and electronically verify PIV or like standard credentials.	L	M	H	
Device Identification and Authentication					
IA-3	The ISO 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	M	H	
Identifier Management					
IA-4	FCPS information systems manage identifiers by: a. Receiving authorization from a designated DTI official to assign an individual, group, role, or device identifier through the approval of a documented naming convention, within the Identification and Authorization Control Procedure. b. Selecting an identifier that uniquely 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. Receiving authorization from a designated DTI official to assign an individual, group, role, or device identifier through the approval of a documented naming convention, within the Identification and Authorization Control Procedure. b. Selecting an identifier that uniquely identifies an individual with supplemental controls provided by the	L	M	H	

	cloud provider to ensure duplicate identifiers are not stored. c. Assigning the user identifier to the intended party. d. Preventing reuse of user identifiers.				
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 FCPS DTI. 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 upon first access or changed/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 to address authentication requirements along with the DTI procedures documented under this security control. Deviations from FCPS DTI Password Management Procedure must be documented and approved by the Authorizing Official. Then	L	M	H	

	approval can be added to the appropriate system security documentation.				
Authenticator Management | Password Based Authentication					
IA-5.1	For password-based authentication, FCPS information systems must: a. Enforce the following minimum password complexity requirements: 1. At least twelve (12) non-blank characters; 2. Characters from three (3) of the following four (4) categories: i. At least one (1) English upper-case characters (A-Z) ii. At least one (1) English lower-case characters (a-z) iii. At least one (1) numbers based on 10 digits (0-9) iv. At least one (1) Non-Alphanumeric/special characters (ex.,!, $, #) b. Enforce at least three (3) changed character rule when new passwords are created c. Store and transmit only encrypted representation of passwords using FISMA compliant valid encryption as defined by NIST standards d. Enforce a password minimum lifetime restriction of two (2) days and a maximum lifetime restriction of 90 days e. 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. f. Prohibit password reuse for a specific account for 24 generations or four (4) years g. Allows the use of a temporary password for system logons, with an immediate change to a permanent password upon first use. h. Password-protect system initialization (boot) settings i. Passwords must not contain: 1. Account Username/unique identifier 2. Beginning or trailing blanks 3. More than two identical characters in a row 4. Recommendations for passwords include avoiding predictability and the following methods and components: i. Common words or phrases ii. Typical topologies (patterns) iii. Initial cap word, followed by number, followed by special character- (e.g., Fall2015!)	L	M	H	

	iv. Special character, number, Cap word (e.g., #1 Redskins) v. Social information vi. Family names, Pet names vii. Telephone numbers, SSNs, Anniversaries, or birthdays. viii. Address, zip code, street name Passwords used on external systems or social websites should never be used for work systems. For public facing systems that require user identification and authentication E-authentication criteria should be used to address authentication requirements along with the FCPS DTI procedures documented under this security control.				
Authenticator Management | PKI Based Authentication					
IA-5.2	For PKI-based authentication, FCPS 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	M	H	
Authenticator Management | In Person or Trusted Third-Party Registration					
IA-5.3	The ISO must require that employees and contractors go through a registration process to receive IDs and tokens. The registration process is carried out in person before a designated registration authority (e.g. ISO, ISSM) with authorization by a designated FCPS official (e.g., a supervisor).	N/A	M	H	
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 FCPS DTI ISSM, that meets the requirements of applicable state and federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	L	M	H	
Authenticator Feedback					
IA-6	All FCPS information systems must obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	L	M	H	
Cryptographic Module Authentication					

IA-7	FCPS information systems must implement mechanisms (compliant with NIST SP 800-52 Rev. 2) 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.	L	M	H	
Identification and Authentication (Non-Organizational Users)					
IA-8	FCPS information systems must uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users). Users are uniquely approved by the ISO, identified and authenticated for all 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.	L	M	H	
Identification and Authentication (Non-Organizational Users) | Acceptance of PIV Credentials from other Agencies					
IA-8.1	FCPS information systems should accept and electronically verify Personal Identity Verification (PIV) or like standard credentials from other federal and state agencies as applicable. This must be explicitly documented within the ISA and Identification & Authorization Procedures for the security boundary.	L	M	H	
Identification and Authentication (Non-Organizational Users) | Acceptance of Third-Party Credentials					
IA-8.2	All FCPS 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.	L	M	H	
Identification and Authentication (Non-Organizational Users) | Use of FICAM Approved Products					
IA-8.3	All FCPS systems employ only FICAM-approved information system components in the FCPS 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.	L	M	H	
Identification and Authentication (Non-Organizational Users) | Use of FICAM Issued Profiles					
IA-8.4	FCPS information systems should conform to FICAM issued profiles as applicable.	L	M	H	

12.5.3.4. System and Communications Control Requirements

Security Control ID	System and Communication Controls	SSecCat Baseline			Status
SC-1	The ISO must develop and implement a System and Communication Protection Procedure, meeting the minimum standards established in the FCPS DTI Procedures, that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance as they pertain to security & risk assessment activities within the organization and describes how ISO intends to implement the security requirements associated with this NIST control family. The System and Communication Protection Procedure must be complimentary to the FCPS DTI guidance and be approved by the FCPS Authorizing Official. **The System and Communication Protection Procedure must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.**	L	M	H	
Application Partitioning					
SC-2	FCPS 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	M	H	
Security Function Isolation					
SC-3	FCPS 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	H	
Information in Shared Resources					
SC-4	The ISO must ensure that information systems prevent unauthorized and unintended information transfer via shared system resources by properly removing data remnants and	N/A	M	H	

	applying least privilege access permissions. See NIST SP 800-66 and SP 800-88 for additional details.				
Denial of Service Protection					
SC-5	The ISO must ensure that information systems protect against or limit the effect of denial of service attacks including directed malicious attacks against FCPS 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).	L	M	H	
Boundary Protection					
SC-7	The ISO 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.	L	M	H	
Boundary Protection | Access Points					

SC-7.3	The ISO 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	M	H	
Boundary Protection | External Telecommunications Services					
SC-7.4	The ISO 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	M	H	
Boundary Protection | Deny by Default/Allow by Exception					
SC-7.5	FCPS 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 ISO manually and/or automatically updates the exception list through a product vendor and/or managed service at least quarterly.	N/A	M	H	
Boundary Protection | Prevent Split Tunneling for Remote Devices					
SC-7.7	FCPS 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	M	H	
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	H	
Boundary Protection | Fail Secure					
SC-7.18	FCPS information systems must fail securely in the event of an operational failure of a boundary protection device.	N/A	N/A	H	

	This enhancement only applies to High categorization systems. If any High systems are introduced in the future, this requirement will be further defined.				
Boundary Protection | Isolation of Information System Components					
SC-7.21	The ISO must employ boundary protection mechanisms to separate FCPS-defined information system components both, physically and logically that support different FCPS-defined missions and/or business functions into security boundaries.	N/A	M	H	
Transmission Confidentiality and Integrity					
SC-8	FCPS information systems must protect the confidentiality and integrity of both internally and externally transmitted information to prevent unauthorized disclosure of Confidential FCPS data and detect changes to information during transmission across the wide area network (WAN) and within the local area network (LAN) as appropriate. FCPS DTI requires the use of valid encryption standards compliant with NIST SP 800-52 Rev.2.	N/A	M	H	
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	M	H	
Network Disconnect					
SC-10	FCPS information systems are to terminate network connections at the end of a session or after 30 minutes of inactivity.	N/A	M	H	
Cryptographic Key Establishment and Management					
SC-12	The ISO 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 IA-5.1. 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,	L	M	H	

	regulations, policies, standards, and guidance including current NIST SP 800 133 and FIPS 140-2.				
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	H	
Cryptographic Protection					
SC-13	When cryptography is employed within information systems, the ISO must ensure the information system implements cryptographic mechanisms that comply with applicable federal laws, Executive Orders, directives, policies, regulations and standards. FCPS 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.	L	M	H	
Collaborative Devices					
SC-15	The ISO 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).	L	M	H	

	NOTE: Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.				
Public Key Infrastructure Certificates					
SC-17	The ISO 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 ISO must also manage the information system trust stores to ensure only approved trust anchors are in the trust stores.	N/A	M	H	
Mobile Code					
SC-18	The ISO must ensure that: a. Acceptable and unacceptable mobile code and mobile code technologies are defined in the System and Communication Protection Procedure. 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	M	H	
Voice Over Internet Protocol (VoIP)					
SC-19	The ISO 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	M	H	
Secure Name/Address Resolution Service (Authoritative Source)					
SC-20	FCPS 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	L	M	H	

	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, must provide other means to assure the authenticity and integrity of response data.				
Secure Name/Address Resolution Service (Recursive or Caching Resolver)					
SC-21	FCPS 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.	L	M	H	
Architecture and Provisioning for Name/Address Resolution Service					
SC-22	The ISO must ensure information systems that collectively provide name/address resolution service for FCPS are fault tolerant and implement internal/external role separation.	L	M	H	
Session Authentication					
SC-23	The ISO 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	M	H	
Fail in Known State					
SC-24	The ISO must ensure that information systems fail to a known secure state for kernel based or whole system failures preserving predefined 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	H	
Protection of Information at Rest					
SC-28	FCPS 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 Confidential/ sensitive data and FTI, while at rest on a storage device or on a secondary storage device like	N/A	M	H	

	a tape drive using FIPS 140-2 cryptographic mechanisms, at a minimum.				
Process Isolation					
SC-39	FCPS 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.	L	M	H	

12.5.3.5. Privacy Controls

12.5.3.5.1. Authority and Purpose

Security Control ID	Authority to Collect Controls	SSecCat Baseline			Status
AP-1	The ISO must determine and document FCPS's legal authority to collect, use, maintain, and share PII, either generally or in support of a specific program or information system requirement. These requirements must be reviewed and updated at least every 3 years and any related procedures reviewed and updated at least annually.	L	M	H	
Purpose Specification					
AP-2	The ISO must describe in its Information Inventories and privacy notices the purpose(s) for which PII is collected, used, maintained, and shared.	N/A	M	H	

12.5.3.5.2. Accountability, Audit, and Risk Management

Security Control ID	Governance and Privacy Program Controls	SSecCat Baseline			Status
AR-1	The ISO must establish a Privacy Program consistent with FCPS Policies, Regulations, Procedures, and NIST Special Publication 800-53 (current revision) requirements.	L	M	H	

	https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final The ISO privacy policy must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.				
Privacy Impact and Risk Assessment					
AR-2	The ISO must: a. Document in the Privacy Impact Assessment (PIA) 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 activities that pose a risk to the privacy of PII.	L	M	H	
Privacy Requirements for Contractors and Service Providers					
AR-3	The ISO must: a. Establish privacy roles, responsibilities, and access requirements for contractors and service providers, documented in the PIA. b. Include privacy requirements in contracts and other acquisition-related documents.	L	M	H	
Privacy Monitoring and Auditing					
AR-4	The ISO must: a. Monitor and audit privacy controls and internal privacy policy as required to ensure effective implementation b. Where applicable, comply with DTI privacy oversight monitoring and auditing policies and procedures	L	M	H	
Privacy Awareness Training					
AR-5	The ISO must: a. Develop, implement, and update a comprehensive privacy, training and awareness strategy aimed at ensuring personnel understand privacy responsibilities and procedures b. 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 FCPS personnel and contractors are required to re-certify and accept privacy training and requirements on an annual basis.	L	M	H	
Privacy Enhanced System Design and Development					
AR-7	The ISO must design information systems that support privacy with automated privacy controls. FCPS DTI requires a focus on implementing the following control families to enhance privacy protection: • Access Control (AC)	L	M	H	

	• Auditing and Accountability (AU) • Identification and Authentication (IA) • System and Communication Protection (SC) • Configuration Management (CM) • System and Information Integrity (SI)				
Accounting of Disclosures					
AR-8	The ISO 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.	L	M	H	

12.5.3.5.3. Data Quality and Integrity

Security Control ID	Data Quality Controls	SSecCat Baseline			Status
DI-1	The ISO 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 d. Issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information The Data Quality process must be reviewed and updated at least every 3 years and all Data Quality procedures reviewed and updated at least annually.	L	M	H	
Validate PII					
DI-1.1	The ISO must request the individual or the individual's authorized representative to validate PII during the collection process.	L	M	H	
Re-Validate PII					
DI-1.2	The ISO must:	L	M	H	

	a. Establish privacy roles, responsibilities, and access requirements for contractors and service providers b. Include privacy requirements in contracts and other acquisition-related documents				
Data Integrity and Data Integrity Board					
DI-2	The ISO must: a. Document processes and procedures to ensure the integrity of PII through existing security controls b. Establish a Data Integrity Board, when appropriate to oversee CMAs, and to ensure those agreements comply with the computer matching provisions of the Privacy Act	L	M	H	

12.5.3.5.4. Data Minimization and Retention

Security Control ID	Data Minimization and Retention Controls	SSecCat Baseline			Status
DM-1	The ISO 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 Information Inventory is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose The inventory must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.	L	M	H	
Minimization of PII/Locate/Remove/Redact/Anonymize PII					
DM-1.1	The ISO 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.	L	M	H	
Data Retention and Disposal					
DM-2	The ISO 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	L	M	H	

	b. 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) and Maryland State Archives-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access c. Use legally compliant techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records). d. Document these procedures within the security boundary's Records Management Plan.				
Data Retention and Disposal/System Configuration					
DM-2.1	The ISO 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.	L	M	H	
Minimization of PII Used in Testing, Training, and Research					
DM-3	The ISO must: a. Adhere to FCPS 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	L	M	H	
Minimization of PII Used in Testing Training, and Research | Risk Minimization Techniques					
DM-3.1	The ISO must, where feasible, use techniques to minimize the risk to privacy of using PII for research, testing, or training.	L	M	H	

12.5.3.5.5. Individual Participation and Redress

Security Control ID	Individual Participation and Redress Controls	SSecCat Baseline			Status
IP-1	The ISO 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	L	M	H	

	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.				
Mechanism Supporting Itemized or Tiered Consent					
IP-1.1	The ISO must implement mechanisms to support itemized or tiered consent for specific uses of data.	L	M	H	
Individual Access					
IP-2	The ISO must: a. Provide individuals the ability to have access to their PII maintained in the system(s) of records b. Publish procedures governing how individuals may request access to records maintained in the system of records c. Adhere to Family Education Rights and Protection Act (FERPA) and Privacy Act requirements and state policies and guidance for the proper processing of Privacy Act request	L	M	H	
Redress					
IP-3	The ISO 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	L	M	H	
Complaint Management					
IP-4	The ISO must implement a process for receiving, documenting, and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.	L	M	H	
Complaint Management | Response Times					
IP-4.1	FCPS must respond to complaints, concerns, and questions from individuals within a 72- hour time period.	L	M	H	

12.5.3.5.6. Security

Security Control ID	Security Controls	SSecCat Baseline			Status
SE-1	The ISO must:	L	M	H	

	a. 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 b. Provide each update of the PII inventory to the FCPS DTI to support the establishment of information security requirements for all new or modified information systems containing PII The information inventory procedures must be reviewed and updated at least every 3 years and the Information Inventory must be reviewed and updated at least annually.				
Privacy Incident Response					
SE-2	The ISO must: a. Develop and implement an Incident Response Plan b. Provide an organized and effective response to privacy incidents in accordance with the security boundary and FCPS DTI 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)	L	M	H	

12.5.3.5.7. Transparency

Security Control ID	Transparency Controls	SSecCat Baseline			Status
TR-1	FCPS 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 FCPS collects and the purpose(s) for which it collects that information	L	M	H	

	2. How FCPS uses PII internally 3. Whether FCPS 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 documentation must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.				
Real Time or Layered Notice					
TR-1.1	The ISO must provide real-time and/or layered notice to individuals at the time when any PII is collected.	L	M	H	
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. If applicable, the ISO must document this information and implementation procedures within the security boundary's Privacy Impact Assessment.	L	M	H	
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 System of Records Notices (SORN) and Privacy Act Statement. If applicable, the ISO must document this information and implementation procedures within the security boundary's Privacy Impact Assessment.	L	M	H	
Dissemination of Privacy Program Information					
TR-3	The ISO 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.	L	M	H	

12.5.3.5.8. Personally Identifiable Information (PII) and Transparency

Security Control ID	Policy and Procedures	SSecCat Baseline			Status
PT-1	a. Develop, document, and disseminate to appropriate system user and administrative groups. 1. System-level personally identifiable information processing and transparency policy that: a). Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b). Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls; b. Designate a FCPS staff member to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency policy and procedures; and c. Review and update the current personally identifiable information processing and transparency: 1. Policy annually and following PII & transparency related BoE Policy and/or Superintendent Regulation changes; and 2. Procedures annually and following any changes to the operational environment necessitating a change in the handling of PII>	L	M	H	
Authority to Process PII					
PT-2	a. Determine and document the legal & operational requirements that permits every step of the information life cycle, including creation, collection, use, processing,	L	M	H	

	storage, maintenance, dissemination, disclosure, and disposal. of personally identifiable information; and b. Restrict every step of the information life cycle, including creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of personally identifiable information to only that which is authorized.				
PII Processing Purposes					
PT-3	a. Identify and document the [Assignment: organization-defined purpose(s)] for processing personally identifiable information; b. Describe the purpose(s) in the public privacy notices and policies of the organization; c. Restrict the [Assignment: organization-defined processing] of personally identifiable information to only that which is compatible with the identified purpose(s); and d. Monitor changes in processing personally identifiable information and implement [Assignment: organization-defined mechanisms] to ensure that any changes are made in accordance with [Assignment: organization-defined requirements]	L	M	H	
PII Processing Purposes | Data Tagging					
PT-3.1	Attach data tags containing the following purposes to [Assignment: organization-defined elements of personally identifiable information]: [Assignment: organization-defined processing purposes].	L	M	H	
PII Processing Purposes | Automation					
PT-3.2	Track processing purposes of personally identifiable information using [Assignment: organization-defined automated mechanisms].	L	M	H	
Consent					
PT-4	Implement [Assignment: organization-defined tools or mechanisms] for individuals to consent to the processing of their personally identifiable information prior to its collection that facilitate individuals' informed decision-making.	L	M	H	
Consent | Tailored Consent					
PT-4.1	Provide [Assignment: organization-defined mechanisms] to allow individuals to tailor processing permissions to selected elements of personally identifiable information.	L	M	H	
Consent | Just-In-Time Consent					
PT-4.2	Present [Assignment: organization-defined consent mechanisms] to individuals at [Assignment: organization-defined frequency] and in conjunction with [Assignment:	L	M	H	

	organization-defined personally identifiable information processing].				
Consent | Revocation					
PT-4.3	Implement [Assignment: organization-defined tools or mechanisms] for individuals to revoke consent to the processing of their personally identifiable information.	L	M	H	
Privacy Notice					
PT-5	Provide notice to individuals about the processing of personally identifiable information that: a. Is available to individuals upon first interacting with an organization, and subsequently at [Assignment: organization-defined frequency]; b. Is clear and easy-to-understand, expressing information about personally identifiable information processing in plain language; c. Identifies the authority that authorizes the processing of personally identifiable information; d. Identifies the purposes for which personally identifiable information is to be processed; and e. Includes [Assignment: organization-defined information].	L	M	H	
Privacy Notice | Just-In-Time Notice					
PT-5.1	Present notice of personally identifiable information processing to individuals at a time and location where the individual provides personally identifiable information or in conjunction with a data action, or [Assignment: organization-defined frequency].	L	M	H	
Privacy Notice | Privacy Statement					
PT-5.2	Include Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.	L	M	H	
System of Records Notice					
PT-6	For systems that process information that will be maintained in a Privacy Act system of records: a. Draft system of records notices in accordance with DTI guidance and submit new and significantly modified system of records notices to the DTI and appropriate congressional committees for advance review; b. Publish system of records notices in the FCPS DTI Security Register; and c. Keep system of records notices accurate, up-to-date, and scoped in accordance with policy.	L	M	H	
System of Record Notice | Routine Uses					
PT-6.1	Review all routine uses published in the system of records notice at [Assignment: organization-defined frequency] to ensure continued accuracy, and to ensure that routine	L	M	H	

	uses continue to be compatible with the purpose for which the information was collected.				
System of Records Notice | Exemption Rules					
PT-6.2	Review all Privacy Act exemptions claimed for the system of records at [Assignment: organization-defined frequency] to ensure they remain appropriate and necessary in accordance with law, that they have been promulgated as regulations, and that they are accurately described in the system of records notice.	L	M	H	
Specific Categories of Personally Identifiable Information					
PT-7	Apply [Assignment: organization-defined processing conditions] for specific categories of personally identifiable information.	L	M	H	
Specific Categories of Personally Identifiable Information | Social Security Numbers					
PT-7.1	When a system processes Social Security numbers: a. Eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to their use as a personal identifier; b. Do not deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his or her Social Security number; and c. Inform any individual who is asked to disclose his or her Social Security number whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.	L	M	H	
Specific Categories of Personally Identifiable Information | First Amendment Info					
PT-7.2	Prohibit the processing of information describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual or unless pertinent to and within the scope of an authorized law enforcement activity.	L	M	H	
Computer Matching Requirements					
PT-8	When a system or organization processes information for the purpose of conducting a matching program: a. Obtain approval from the AO to conduct the matching program; b. Develop and enter into a computer matching agreement; c. Publish a matching notice in the FCPS DTI Security Register; d. Independently verify the information produced by the matching program before taking adverse action against an individual, if required; and	L	M	H	

	e. Provide individuals with notice and an opportunity to contest the findings before taking adverse action against an individual.				

12.5.3.5.9. Use Limitation

Security Control ID	Use Limitation Controls	SSecCat Baseline			Status
UL-1	The ISO must use PII internally only for the authorized purpose(s) identified in the Privacy Impact Assessment and/or in public notices. The process must be reviewed and updated at least every 3 years and the procedures reviewed and updated at least annually.	L	M	H	
Information Sharing with Third Parties					
UL-2	The ISO must: a. Share PII externally, only for the authorized purposes identified in the PIA and/or described in its notice(s) or for a purpose that is compatible with those purposes b. 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 c. Monitor, audit, and train staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII d. 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.	L	M	H	

12.6. Information System Security Inventory of PII & FCPS Confidential Data

The system security inventory documents all automated information systems associated within a security boundary that contains PII (Staff & Student) & FCPS Sensitive Information.

Examples of assets associated with automated information systems that contain PII include:

- Information assets: databases and data files, system documentation, user manuals, training material, 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

A complete inventory shall include a unique system name, a system owner, a staff/student classification and and a description of the physical location of the asset.

Number	Unique Name of information system containing PII	Information Owner (Name and Title)	Staff/Student Classification	Description of the Service the System Supports	Date of Most Recent System Authorization (ex. Authorization to Operate, etc.)	Location of System *(Include externally hosted systems as well as assets containing system backups)*
1.						
2.						

12.7. Inventory of Records Containing PII & FCPS Confidential Data

The Records Inventory documents all records associated within a security boundary that contains PII (Staff & Student).

Records that can contain PII & FCPS Sensitive Information are defined as:

- A record is any documentary material created or received by an organization in connection with the transaction of public business.
- A common misconception exists that all records are on paper. In actuality, electronic documentation is as much a record as paper documentation and should be treated as such. This can include minutes typed on computers, email, spreadsheets, databases, and websites.
- As a rule, assume that content and function, rather than format, determine whether an item is a record and how long it should be kept.

A complete inventory shall include a unique Record Series name, an information owner, a staff/student classification and a description of the physical location of the Record.

Number	Unique Record Series Name containing PII & FCPS Sensitive Information	Information Owner (Name and Title)	Staff/Student Classification	Description of the Record	Retention Schedule (ex. MSA forms DGS 550-14 & DGS 550-15, etc.)	Location Record Storage
1.						
2.						

12.8. FCPS Data Collection & Disclosure Inventory

The ISO must complete the *FCPS Data Collection Inventory.xlsx* for each database, within the security boundary, used to collection FCPS information.

Table Revision Date	Data Store Name	Database Type	On Premise/Cloud	Data Store Location	Number of Records Contained within Database	3rd Party Application Integration	At Rest Encryption	Licensing Model	Price	Quantity	Cost	Period of Performance	Accounts with Administrative Access	Administrative Access Method	Authorized User Groups	User Access Method	User Interaction Method	Purpose of Data Collection (Administrative, Assessment, Instructional, Operational)	Description of Collection Requirement

First Initial	First Name	Middle Initial	Middle Name	Last Name	Home Address	Employee ID	Social Security Number	Position Title	Financial Information	Work Location	Leave Information	Background Investigation Results	Disciplinary Information	Health Information	School Name or School ID	School Address	Teacher Name or Teacher ID	Course	Grade	Gender	Date of Birth	Race	Ethnicity	Language	FARMS Status	ELL Status	IEP/Special Ed Status	504 Status	Student Address	Student Email	Student Phone	Guardian Name	Guardian Phone	Guardian Email Address	Student User Name	Student Password	FCPS Student ID Number	MD State Student ID Number	Photo	Add Fields If Not Listed

The ISO must also complete the *FCPS Data Sharing Disclosure.xlsx* for each information system, which receives information from a database within the security boundary.

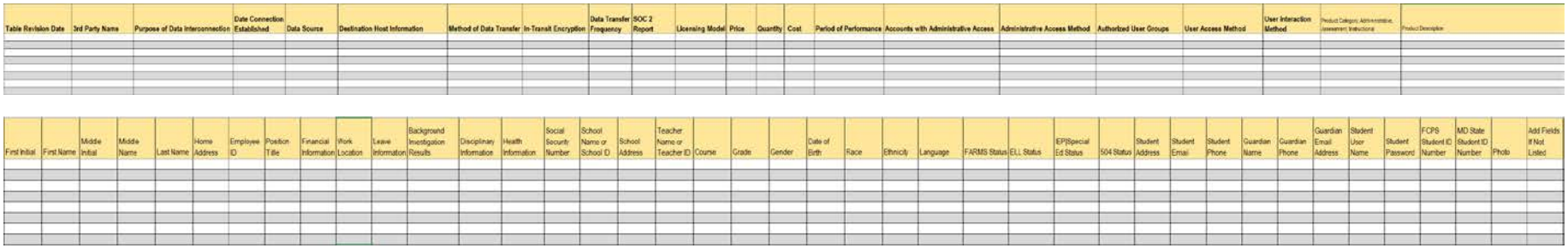


Table Revision Date	3rd Party Name	Purpose of Data Interconnection	Date Connection Established	Data Source	Destination Host Information	Method of Data Transfer	In-Transit Encryption	Data Transfer Frequency	SOC 2 Report	Licensing Model	Price	Quantity	Cost	Period of Performance	Accounts with Administrative Access	Administrative Access Method	Authorized User Groups	User Access Method	User Interaction Method	Product Category (Administrative, Assessment, Instructional)	Product Description

First Initial	First Name	Middle Initial	Middle Name	Last Name	Home Address	Employee ID	Position Title	Financial Information	Work Location	Leave Information	Background Investigation Results	Disciplinary Information	Health Information	Social Security Number	School Name or School ID	School Address	Teacher Name or Teacher ID	Course	Grade	Gender	Date of Birth	Race	Ethnicity	Language	FARMS Status	ELL Status	IEP/Special Ed Status	504 Status	Student Address	Student Email	Student Phone	Guardian Name	Guardian Phone	Guardian Email Address	Student User Name	Student Password	FCPS Student ID Number	MD State Student ID Number	Photo	Add Fields If Not Listed

The *FCPS Data Collection Inventory.xlsx* & the *FCPS Data Sharing Disclosure.xlsx* have been shared with the ISO via FCPS SharePoint, at the time this document was provided.

13 Appendix B: Maryland DoIT Incident Reporting Form

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:	

14 Appendix C: HIPAA/NIST/COBIT 5/ISA/ISO Crosswalk

The National Institute of Standards and Technology (NIST) maintains the preferred Framework for government organizations to Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) as directed in Executive Order 13636, Improving Critical Infrastructure Cybersecurity. The Cybersecurity Framework provides a risk-based approach—based on existing standards, guidelines, and practices—to help organizations in any industry to understand, communicate, and manage cybersecurity risks. In the health care space, entities (covered entities and business associates) regulated by the Health Insurance Portability and Accountability Act (HIPAA) must comply with the HIPAA Security Rule to ensure the confidentiality, integrity, and availability of electronic protected health information (ePHI) that they create, receive, maintain, or transmit. This crosswalk document identifies "mappings" between the Cybersecurity Framework and the HIPAA Security Rule.

Organizations that have already aligned their security programs to either the NIST Cybersecurity Framework or the HIPAA Security Rule may find this crosswalk helpful as a starting place to identify potential gaps in their programs. Addressing these gaps can bolster their compliance with the Security Rule and improve their ability to secure ePHI and other critical information and business processes. For example, if a covered entity has an existing security program aligned to the HIPAA Security Rule, the entity can use this mapping document to identify which pieces of the NIST Cybersecurity Framework it is already meeting and which represent new practices to incorporate into its risk management program. This mapping document also allows organizations to communicate activities and outcomes internally and externally regarding their cybersecurity program by utilizing the Cybersecurity Framework as a common language. Finally, the mapping can be easily combined with similar mappings to account for additional organizational considerations (e.g., privacy, regulation and legislation). Additional resources, including a FAQ and overview, are available to assist organizations with the use and implementation of the NIST Cybersecurity Framework.

This crosswalk maps each administrative, physical and technical safeguard standard and implementation specification[5] in the HIPAA Security Rule to a relevant NIST Cybersecurity Framework Subcategory. Due to the granularity of the NIST Cybersecurity Framework's Subcategories, some HIPAA Security Rule requirements may map to more than one Subcategory. Activities to be performed for a particular Subcategory of the NIST Cybersecurity Framework may be more specific and detailed than those performed for the mapped HIPAA Security Rule requirement. However, the HIPAA Security Rule is designed to be flexible, scalable and technology-neutral, which enables it to accommodate integration with frameworks such as the NIST Cybersecurity Framework. A HIPAA covered entity or business

[5] Although all Security Rule administrative, physical, and technical safeguards map to at least one of the NIST Cybersecurity Framework Subcategories, other Security Rule standards, such as specific requirements for documentation and organization, do not. HIPAA covered entities and business associates cannot rely entirely on the crosswalk for compliance with the Security Rule.

associate should be able to assess and implement new and evolving technologies and best practices that it determines would be reasonable and appropriate to ensure the confidentiality, integrity and availability of the ePHI it creates, receives, maintains, or transmits.

The mappings between the Framework subcategories and the HIPAA Security Rule are intended to be an informative reference and do not imply or guarantee compliance with any laws or regulations. Users who have aligned their security program to the NIST Cybersecurity Framework should not assume that by so doing they are in full compliance with the Security Rule. Conversely, the HIPAA Security Rule does not require covered entities to integrate the Cybersecurity Framework into their security management programs. Covered entities and business associates should perform their own security risk analyses to identify and mitigate threats to the ePHI they create, receive, maintain or transmit. Whether starting a new security program or reviewing an existing one, organizations will want to visit OCR's Security Rule compliance guidance; HealthIT.gov for resources on cybersecurity, security risk assessments, security training; as well as the FDA's guidance on cybersecurity for medical devices. To find assistance with the use and implementation of the NIST Cybersecurity Framework, organizations may explore the C-Cubed Voluntary Program and NIST's frequently asked questions.

The table below incorporates mappings of HIPAA Security Rule standards and implementation specifications to applicable NIST Cybersecurity Framework Subcategories. These mappings are included in the "Relevant Control Mappings" column which also includes mappings from other security frameworks. The other columns ("Function", "Category", and "Subcategory") correlate directly to the Function, Category and Subcategory Unique Identifiers defined within the NIST Cybersecurity Framework. Other frameworks included in the mapping to the NIST Cybersecurity Framework include: the Council on Cybersecurity Critical Security Controls (CCS CSC); Control Objectives for Information and Related Technology Edition 5 (COBIT 5); International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) 27001; International Society of Automation (ISA) 62443; National Institute of Standards and Technology (NIST) SP 800-53 Rev. 4.

Function	Category	Subcategory	Relevant Control Mappings[2]
	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	• CCS CSC 1 • COBIT 5 BAI09.01, BAI09.02 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.310(a)(2)(ii), 164.310(d)
		ID.AM-2: Software platforms and applications within the organization are inventoried	• CCS CSC 2 • COBIT 5 BAI09.01, BAI09.02, BAI09.05 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(7)(ii)(E)
		ID.AM-3: Organizational communication and data flows are mapped	• CCS CSC 1 • COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.2.3.4 • ISO/IEC 27001:2013 A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(3)(ii)(A), 164.308(a)(8), 164.310(d)

Function	Category	Subcategory	Relevant Control Mappings[2]
		ID.AM-4: External information systems are catalogued	• COBIT 5 APO02.02 • ISO/IEC 27001:2013 A.11.2.6 • NIST SP 800-53 Rev. 4 AC-20, SA-9 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(4)(ii)(A), 164.308(b), 164.314(a)(1), 164.314(a)(2)(i)(B), 164.314(a)(2)(ii), 164.316(b)(2)
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	• COBIT 5 APO03.03, APO03.04, BAI09.02 • ISA 62443-2-1:2009 4.2.3.6 • ISO/IEC 27001:2013 A.8.2.1 • NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(7)(ii)(E)
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	• COBIT 5 APO01.02, DSS06.03 • ISA 62443-2-1:2009 4.3.2.3.3 • ISO/IEC 27001:2013 A.6.1.1 • NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(2), 164.308(a)(3), 164.308(a)(4), 164.308(b)(1), 164.314

Function	Category	Subcategory	Relevant Control Mappings[2]
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	• COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 • ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2 • NIST SP 800-53 Rev. 4 CP-2, SA-12 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(4)(ii), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(2)(i), 164.314, 164.316
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	• COBIT 5 APO02.06, APO03.01 • NIST SP 800-53 Rev. 4 PM-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(4)(ii), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(2)(i), 164.314, 164.316
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	• COBIT 5 APO02.01, APO02.06, APO03.01 • ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 • NIST SP 800-53 Rev. 4 PM-11, SA-14 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E), 164.310(a)(2)(i), 164.316

Function	Category	Subcategory	Relevant Control Mappings[2]
IDENTIFY (ID)		**ID.BE-4:** Dependencies and critical functions for delivery of critical services are established	• ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 • NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(i), 164.308.(a)(7)(ii)(E), 164.310(a)(2)(i), 164.312(a)(2)(ii), 164.314(a)(1), 164.314(b)(2)(i)
		ID.BE-5: Resilience requirements to support delivery of critical services are established	• COBIT 5 DSS04.02 • ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 • NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(B), 164.308(a)(6)(ii), 164.308(a)(7), 164.308(a)(8), 164.310(a)(2)(i), 164.312(a)(2)(ii), 164.314(b)(2)(i)
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established	• COBIT 5 APO13.12 • ISA 62443-2-1:2009 4.3.2.3.3 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.1 • NIST SP 800-53 Rev. 4 PM-1, PS-7 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(i), 164.316
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	• COBIT 5 APO13.12 • ISA 62443-2-1:2009 4.3.2.3.3 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.1 • NIST SP 800-53 Rev. 4 PM-1, PS-7 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(2), 164.308(a)(3), 164.308(a)(4), 164.308(b), 164.314

Function	Category	Subcategory	Relevant Control Mappings[2]
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	• COBIT 5 MEA03.01, MEA03.04 • ISA 62443-2-1:2009 4.4.3.7 • ISO/IEC 27001:2013 A.18.1 • NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1) • HIPAA Security Rule 45 C.F.R. §§ 164.306, 164.308, 164.310, 164.312, 164.314, 164.316
		ID.GV-4: Governance and risk management processes address cybersecurity risks	• COBIT 5 DSS04.02 • ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 • NIST SP 800-53 Rev. 4 PM-9, PM-11 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1), 164.308(b)
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	• CCS CSC 4 • COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 • ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 • ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 • NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.312(a)(1), 164.316(b)(2)(iii)

Function	Category	Subcategory	Relevant Control Mappings[2]
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	• ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 • ISO/IEC 27001:2013 A.6.1.4 • NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5 • No direct analog to HIPAA Security Rule[3]
		ID.RA-3: Threats, both internal and external, are identified and documented	• COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 • ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 • NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(A), 164.310(a)(1), 164.310(a)(2)(iii), 164.312(a)(1), 164.312(c), 164.312(e), 164.314, 164.316
		ID.RA-4: Potential business impacts and likelihoods are identified	• COBIT 5 DSS04.02 • ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 • NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(6), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.316(a)

Function	Category	Subcategory	Relevant Control Mappings[2]
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	• COBIT 5 APO12.02 • ISO/IEC 27001:2013 A.12.6.1 • NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E), 164.316(a)
		ID.RA-6: Risk responses are identified and prioritized	• COBIT 5 APO12.05, APO13.02 • NIST SP 800-53 Rev. 4 PM-4, PM-9 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(B), 164.314(a)(2)(i)(C), 164.314(b)(2)(iv)
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	• COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 • ISA 62443-2-1:2009 4.3.4.2 • NIST SP 800-53 Rev. 4 PM-9 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(1)(ii)(B)
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	• COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.3.2.6.5 • NIST SP 800-53 Rev. 4 PM-9 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(1)(ii)(B)

Function	Category	Subcategory	Relevant Control Mappings[2]
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	• NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(B), 164.308(a)(6)(ii), 164.308(a)(7)(i), 164.308(a)(7)(ii)(C),164.308(a)(7)(ii)(E), 164.310(a)(2)(i)
	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	• CCS CSC 16 • COBIT 5 DSS05.04, DSS06.03 • ISA 62443-2-1:2009 4.3.3.5.1 • ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 • ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 • NIST SP 800-53 Rev. 4 AC-2, IA Family • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(d)

Function	Category	Subcategory	Relevant Control Mappings[2]
		PR.AC-2: Physical access to assets is managed and protected	• COBIT 5 DSS01.04, DSS05.05 • ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 • ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 • NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(B), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.310(a)(1), 164.310(a)(2)(i), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii)
		PR.AC-3: Remote access is managed	• COBIT 5 APO13.01, DSS01.04, DSS05.03 • ISA 62443-2-1:2009 4.3.3.6.6 • ISA 62443-3-3:2013 SR 1.13, SR 2.6 • ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1 • NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(4)(i), 164.308(b)(1), 164.308(b)(3), 164.310(b), 164.312(e)(1), 164.312(e)(2)(ii)

Function	Category	Subcategory	Relevant Control Mappings[2]
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	• CCS CSC 12, 15 • ISA 62443-2-1:2009 4.3.3.7.3 • ISA 62443-3-3:2013 SR 2.1 • ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 • NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3), 164.308(a)(4), 164.310(a)(2)(iii), 164.310(b), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii)
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	• ISA 62443-2-1:2009 4.3.3.4 • ISA 62443-3-3:2013 SR 3.1, SR 3.8 • ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, SC-7 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(4)(ii)(B), 164.310(a)(1), 164.310(b), 164.312(a)(1), 164.312(b), 164.312(c), 164.312(e)

Function	Category	Subcategory	Relevant Control Mappings[2]
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	• CCS CSC 9 • COBIT 5 APO07.03, BAI05.07 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.7.2.2 • NIST SP 800-53 Rev. 4 AT-2, PM-13 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(5)
		PR.AT-2: Privileged users understand roles & responsibilities	• CCS CSC 9 • COBIT 5 APO07.02, DSS06.03 • ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • NIST SP 800-53 Rev. 4 AT-3, PM-13 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(2), 164.308(a)(3)(i), 164.308(a)(5)(i), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(5)(ii)(D)
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	• CCS CSC 9 • COBIT 5 APO07.03, APO10.04, APO10.05 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • NIST SP 800-53 Rev. 4 PS-7, SA-9 • HIPAA Security Rule 45 C.F.R. §§ 164.308(b), 164.314(a)(1), 164.314(a)(2)(i), 164.314(a)(2)(ii)

Function	Category	Subcategory	Relevant Control Mappings[2]
		PR.AT-4: Senior executives understand roles & responsibilities	• CCS CSC 9 • COBIT 5 APO07.03 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, • NIST SP 800-53 Rev. 4 AT-3, PM-13 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(2), 164.308(a)(3)(i), 164.308(a)(5)(i), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(5)(ii)(D)
		PR.AT-5: Physical and information security personnel understand roles & responsibilities	• CCS CSC 9 • COBIT 5 APO07.03 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, • NIST SP 800-53 Rev. 4 AT-3, PM-13 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(2), 164.308(a)(3)(i), 164.308(a)(5)(i), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(5)(ii)(D), 164.530(b)(1)
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	• CCS CSC 17 • COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06 • ISA 62443-3-3:2013 SR 3.4, SR 4.1 • ISO/IEC 27001:2013 A.8.2.3 • NIST SP 800-53 Rev. 4 SC-28 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(b)(1), 164.310(d), 164.312(a)(1), 164.312(a)(2)(iii), 164.312(a)(2)(iv), 164.312(b), 164.312(c), 164.314(b)(2)(i), 164.312(d)

Function	Category	Subcategory	Relevant Control Mappings[2]
		PR.DS-2: Data-in-transit is protected	• CCS CSC 17 • COBIT 5 APO01.06, DSS06.06 • ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 • ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 • NIST SP 800-53 Rev. 4 SC-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(b)(1), 164.308(b)(2), 164.312(e)(1), 164.312(e)(2)(i), 164.312(e)(2)(ii), 164.314(b)(2)(i)
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	• COBIT 5 BAI09.03 • ISA 62443-2-1:2009 4. 4.3.3.3.9, 4.3.4.4.1 • ISA 62443-3-3:2013 SR 4.2 • ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 • NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(d)(1), 164.310(d)(2)
		PR.DS-4: Adequate capacity to ensure availability is maintained	• COBIT 5 APO13.01 • ISA 62443-3-3:2013 SR 7.1, SR 7.2 • ISO/IEC 27001:2013 A.12.3.1 • NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(7), 164.310(a)(2)(i), 164.310(d)(2)(iv), 164.312(a)(2)(ii)

Function	Category	Subcategory	Relevant Control Mappings[2]
		PR.DS-5: Protections against data leaks are implemented	• CCS CSC 17 • COBIT 5 APO01.06 • ISA 62443-3-3:2013 SR 5.2 • ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 • NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.310(b), 164.310(c), 164.312(a), 164.312(e)
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	• ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8 • ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 • NIST SP 800-53 Rev. 4 SI-7 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.312(b), 164.312(c)(1), 164.312(c)(2), 164.312(e)(2)(i)

Function	Category	Subcategory	Relevant Control Mappings[2]
PROTECT		**PR.DS-7:** The development and testing environment(s) are separate from the production environment	• COBIT 5 BAI07.04 • ISO/IEC 27001:2013 A.12.1.4 • NIST SP 800-53 Rev. 4 CM-2 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(4)[4]
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	• CCS CSC 3, 10 • COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 • ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 • ISA 62443-3-3:2013 SR 7.6 • ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(8), 164.308(a)(7)(i), 164.308(a)(7)(ii)

Function	Category	Subcategory	Relevant Control Mappings[2]
(PR)		**PR.IP-2:** A System Development Life Cycle to manage systems is implemented	• COBIT 5 APO13.01 • ISA 62443-2-1:2009 4.3.4.3.3 • ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 • NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(1)(i)
		PR.IP-3: Configuration change control processes are in place	• COBIT 5 BAI06.01, BAI01.06 • ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 • ISA 62443-3-3:2013 SR 7.6 • ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(8)
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	• COBIT 5 APO13.01 • ISA 62443-2-1:2009 4.3.4.3.9 • ISA 62443-3-3:2013 SR 7.3, SR 7.4 • ISO/IEC 27001:2013 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3 • NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(D), 164.310(a)(2)(i), 164.310(d)(2)(iv)

Function	Category	Subcategory	Relevant Control Mappings[2]
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	• COBIT 5 DSS01.04, DSS05.05 • ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 • ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 • NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(i), 164.308(a)(7)(ii)(C), 164.310, 164.316(b)(2)(iii)
		PR.IP-6: Data is destroyed according to policy	• COBIT 5 BAI09.03 • ISA 62443-2-1:2009 4.3.4.4.4 • ISA 62443-3-3:2013 SR 4.2 • ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 • NIST SP 800-53 Rev. 4 MP-6 • HIPAA Security Rule 45 C.F.R. §§ 164.310(d)(2)(i), 164.310(d)(2)(ii)
		PR.IP-7: Protection processes are continuously improved	• COBIT 5 APO11.06, DSS04.05 • ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 • NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6 • HIPAA Security Rule 45 C.F.R. §§ 164.306(e), 164.308(a)(7)(ii)(D), 164.308(a)(8), 164.316(b)(2)(iii)

Function	Category	Subcategory	Relevant Control Mappings[2]
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	• ISO/IEC 27001:2013 A.16.1.6 • NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(ii)
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	• COBIT 5 DSS04.03 • ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1 • ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2 • NIST SP 800-53 Rev. 4 CP-2, IR-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(6), 164.308(a)(7), 164.310(a)(2)(i), 164.312(a)(2)(ii)
		PR.IP-10: Response and recovery plans are tested	• ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 • ISA 62443-3-3:2013 SR 3.3 • ISO/IEC 27001:2013 A.17.1.3 • NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(7)(ii)(D)
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	• COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 • ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 • ISO/IEC 27001:2013 A.7.1.1, A.7.3.1, A.8.1.4 • NIST SP 800-53 Rev. 4 PS Family • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(C), 164.308(a)(3)

Function	Category	Subcategory	Relevant Control Mappings[2]
		PR.IP-12: A vulnerability management plan is developed and implemented	• ISO/IEC 27001:2013 A.12.6.1, A.18.2.2 • NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B)
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	• COBIT 5 BAI09.03 • ISA 62443-2-1:2009 4.3.3.3.7 • ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5 • NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3)(ii)(A), 164.310(a)(2)(iv)

Function	Category	Subcategory	Relevant Control Mappings[2]
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	• COBIT 5 DSS05.04 • ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 • ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 • NIST SP 800-53 Rev. 4 MA-4 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3)(ii)(A), 164.310(d)(1), 164.310(d)(2)(ii), 164.310(d)(2)(iii), 164.312(a), 164.312(a)(2)(ii), 164.312(a)(2)(iv), 164.312(b), 164.312(d), 164.312(e), 164.308(a)(1)(ii)(D)

Function	Category	Subcategory	Relevant Control Mappings[2]
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	• CCS CSC 14 • COBIT 5 APO11.04 • ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 • ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 • ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 • NIST SP 800-53 Rev. 4 AU Family • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.310(a)(2)(iv), 164.310(d)(2)(iii), 164.312(b)
		PR.PT-2: Removable media is protected and its use restricted according to policy	• COBIT 5 DSS05.02, APO13.01 • ISA 62443-3-3:2013 SR 2.3 • ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 • NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3)(i), 164.308(a)(3)(ii)(A), 164.310(d)(1), 164.310(d)(2), 164.312(a)(1), 164.312(a)(2)(iv), 164.312(b)

Function	Category	Subcategory	Relevant Control Mappings[2]
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	• COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 • ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 • ISO/IEC 27001:2013 A.9.1.2 • NIST SP 800-53 Rev. 4 AC-3, CM-7 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3), 164.308(a)(4), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iv)
		PR.PT-4: Communications and control networks are protected	• CCS CSC 7 • COBIT 5 DSS05.02, APO13.01 • ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 • ISO/IEC 27001:2013 A.13.1.1, A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.312(a)(1), 164.312(b), 164.312(e)

Function	Category	Subcategory	Relevant Control Mappings[2]
	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	• COBIT 5 DSS03.01 • ISA 62443-2-1:2009 4.4.3.3 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.312(b)
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	• ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 • ISO/IEC 27001:2013 A.16.1.1, A.16.1.4 • NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4 • HIPAA Security Rule 45 C.F.R. § 164.308(6)(i)
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	• ISA 62443-3-3:2013 SR 6.1 • NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(ii), 164.308(a)(8), 164.310(d)(2)(iii), 164.312(b), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii)
		DE.AE-4: Impact of events is determined	• COBIT 5 APO12.06 • NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI-4 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(ii)

Function	Category	Subcategory	Relevant Control Mappings[2]
		DE.AE-5: Incident alert thresholds are established	• COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.2.3.10 • NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(i)
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	• CCS CSC 14, 16 • COBIT 5 DSS05.07 • ISA 62443-3-3:2013 SR 6.2 • NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(8), 164.312(b), 164.312(e)(2)(i)
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	• ISA 62443-2-1:2009 4.3.3.3.8 • NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20 • HIPAA Security Rule 45 C.F.R. §§ 164.310(a)(2)(ii), 164.310(a)(2)(iii)

Function	Category	Subcategory	Relevant Control Mappings[2]
DETECT (DE)		**DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events	• ISA 62443-3-3:2013 SR 6.2 • ISO/IEC 27001:2013 A.12.4.1 • NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(3)(ii)(A), 164.308(a)(5)(ii)(C), 164.312(a)(2)(i), 164.312(b), 164.312(d), 164.312(e)
		DE.CM-4: Malicious code is detected	• CCS CSC 5 • COBIT 5 DSS05.01 • ISA 62443-2-1:2009 4.3.4.3.8 • ISA 62443-3-3:2013 SR 3.2 • ISO/IEC 27001:2013 A.12.2.1 • NIST SP 800-53 Rev. 4 SI-3 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B)
		DE.CM-5: Unauthorized mobile code is detected	• ISA 62443-3-3:2013 SR 2.4 • ISO/IEC 27001:2013 A.12.5.1 • NIST SP 800-53 Rev. 4 SC-18, SI-4. SC-44 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B)
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	• COBIT 5 APO07.06 • ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 • NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(1)(ii)(D)

Function	Category	Subcategory	Relevant Control Mappings[2]
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	• NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii), 164.312(b), 164.314(b)(2)(i)
		DE.CM-8: Vulnerability scans are performed	• COBIT 5 BAI03.10 • ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 • ISO/IEC 27001:2013 A.12.6.1 • NIST SP 800-53 Rev. 4 RA-5 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(8)
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	• CCS CSC 5 • COBIT 5 DSS05.01 • ISA 62443-2-1:2009 4.4.3.1 • ISO/IEC 27001:2013 A.6.1.1 • NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(2), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(4), 164.310(a)(2)(iii), 164.312(a)(1), 164.312(a)(2)(ii)

Function	Category	Subcategory	Relevant Control Mappings[2]
		DE.DP-2: Detection activities comply with all applicable requirements	• ISA 62443-2-1:2009 4.4.3.2 • ISO/IEC 27001:2013 A.18.1.4 • NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(8)
		DE.DP-3: Detection processes are tested	• COBIT 5 APO13.02 • ISA 62443-2-1:2009 4.4.3.2 • ISA 62443-3-3:2013 SR 3.3 • ISO/IEC 27001:2013 A.14.2.8 • NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4 • HIPAA Security Rule 45 C.F.R. § 164.306(e)
		DE.DP-4: Event detection information is communicated to appropriate parties	• COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.3.4.5.9 • ISA 62443-3-3:2013 SR 6.1 • ISO/IEC 27001:2013 A.16.1.2 • NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(6)(ii), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii)
		DE.DP-5: Detection processes are continuously improved	• COBIT 5 APO11.06, DSS04.05 • ISA 62443-2-1:2009 4.4.3.4 • ISO/IEC 27001:2013 A.16.1.6 • NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14 • HIPAA Security Rule 45 C.F.R. §§ 164.306(e), 164.308(a)(8)

Function	Category	Subcategory	Relevant Control Mappings[2]
	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event	• COBIT 5 BAI01.10 • CCS CSC 18 • ISA 62443-2-1:2009 4.3.4.5.1 • ISO/IEC 27001:2013 A.16.1.5 • NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(6)(ii), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.310(a)(2)(i), 164.312(a)(2)(ii)
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	• ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 • ISO/IEC 27001:2013 A.6.1.1, A.16.1.1 • NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(2), 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.310(a)(2)(i), 164.308(a)(6)(i), 164.312(a)(2)(ii)
		RS.CO-2: Events are reported consistent with established criteria	• ISA 62443-2-1:2009 4.3.4.5.5 • ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 • NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(ii), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii)

Function	Category	Subcategory	Relevant Control Mappings[2]
		RS.CO-3: Information is shared consistent with response plans	• ISA 62443-2-1:2009 4.3.4.5.2 • ISO/IEC 27001:2013 A.16.1.2 • NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(ii), 164.314(a)(2)(i)(C)
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	• ISA 62443-2-1:2009 4.3.4.5.5 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(6), 164.308(a)(7), 164.310(a)(2)(i), 164.312(a)(2)(ii)
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	• NIST SP 800-53 Rev. 4 PM-15, SI-5 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)

Function	Category	Subcategory	Relevant Control Mappings[2]
RESPOND (RS)	**Analysis (RS.AN):** Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	• COBIT 5 DSS02.07 • ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • ISA 62443-3-3:2013 SR 6.1 • ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 • NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(ii), 164.312(b)
		RS.AN-2: The impact of the incident is understood	• ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • ISO/IEC 27001:2013 A.16.1.6 • NIST SP 800-53 Rev. 4 CP-2, IR-4 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(6)(ii), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(E)
		RS.AN-3: Forensics are performed	• ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 • ISO/IEC 27001:2013 A.16.1.7 • NIST SP 800-53 Rev. 4 AU-7, IR-4 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)
		RS.AN-4: Incidents are categorized consistent with response plans	• ISA 62443-2-1:2009 4.3.4.5.6 • ISO/IEC 27001:2013 A.16.1.4 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(ii)

Function	Category	Subcategory	Relevant Control Mappings[2]
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained	• ISA 62443-2-1:2009 4.3.4.5.6 • ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 • ISO/IEC 27001:2013 A.16.1.5 • NIST SP 800-53 Rev. 4 IR-4 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(ii)
		RS.MI-2: Incidents are mitigated	• ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 • ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 • NIST SP 800-53 Rev. 4 IR-4 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(ii)
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	• ISO/IEC 27001:2013 A.12.6.1 • NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(6)(ii)
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	• COBIT 5 BAI01.13 • ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 • ISO/IEC 27001:2013 A.16.1.6 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(ii)(D), 164.308(a)(8), 164.316(b)(2)(iii))
		RS.IM-2: Response strategies are updated	• NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(ii)(D), 164.308(a)(8)
	Recovery Planning (RC.RP): Recovery	**RC.RP-1:** Recovery	• CCS CSC 8

Function	Category	Subcategory	Relevant Control Mappings[2]
	processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	plan is executed during or after an event	• COBIT 5 DSS02.05, DSS03.04 • ISO/IEC 27001:2013 A.16.1.5 • NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7), 164.310(a)(2)(i)
RECOVER (RC)	**Improvements (RC.IM):** Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	• COBIT 5 BAI05.07 • ISA 62443-2-1:2009 4.4.3.4 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(ii)(D), 164.308(a)(8), 164.316(b)(2)(iii)
		RC.IM-2: Recovery strategies are updated	• COBIT 5 BAI07.08 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(ii)(D), 164.308(a)(8)
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and	**RC.CO-1:** Public relations are managed	• COBIT 5 EDM03.02 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(i)[5]
		RC.CO-2: Reputation after an event is repaired	• COBIT 5 EDM03.02 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(i)[5]

Function	Category	Subcategory	Relevant Control Mappings[2]
	vendors.	**RC.CO-3:** Recovery activities are communicated to internal stakeholders and executive and management teams	• NIST SP 800-53 Rev. 4 CP-2, IR-4 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(6)(ii), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.310(a)(2)(i), 164.314(a)(2)(i)(C)

15 Appendix D: PCI DSS/NIST/CIS CSC/COBIT 5/ISA/ISO Crosswalk

The Payment Card Industry Data Security Standard (PCI DSS) and the National Institute of Standards and Technology's (NIST) Cybersecurity Framework ("the NIST Framework") share the common goal of enhancing data security. This document, created by the PCI Security Standards Council (PCI SSC), maps PCI DSS to the NIST Framework and provides a resource for stakeholders to use in understanding how to align security efforts to meet objectives in both PCI DSS and the NIST Framework

PCI DSS is focused on the unique security threats and risks present in the payments industry. It defines security requirements for the protection of payment card data, as well as validation procedures and guidance to help organizations understand the intent of the requirements. PCI SSC works with merchants, service providers, financial institutions, technology vendors, and others in the payments industry, as well as our assessor and forensic investigator communities. This keeps all stakeholders aware of current risks to payment data and ensures that PCI Standards continue to address those risks.

The NIST Framework provides an overarching security and risk-management structure for voluntary use by U.S. critical infrastructure owners and operators. The NIST Framework core components consists of security Functions, Categories, and Subcategories of actions. These Subcategories reference globally recognized standards for cybersecurity. As the NIST Framework is broadly focused on organizational risk management, achieving the outcomes stated therein does not provide assurance that payment data is also protected.

Both PCI DSS and the NIST Framework are solid security approaches that address common security goals and principles as relevant to specific risks. While the NIST Framework identifies general security outcomes and activities, PCI DSS provides specific direction and guidance on how to meet security outcomes for payment environments. Because PCI DSS and the NIST Framework are intended for different audiences and uses, they are not interchangeable, and neither one is a replacement for the other.

This mapping is based on PCI DSS v3.2.1 and the Cybersecurity Framework v1.1, using the 2018-04-16_framework_v.1.1_core" spreadsheet1. PCI SSC evaluated each NIST Framework outcome (for example, ID.AM-1) against PCI DSS requirements and identified the relevant PCI DSS requirements for each outcome. The resultant mapping shows where the NIST Framework and PCI DSS contribute to the same security outcomes. PCI DSS requirements that map to an outcome are noted as "Informative References" in blue in the table below.

The mapping covers all NIST Framework Functions and Categories, with PCI DSS requirements directly mapping to 96 of the 108 Subcategories. The mapping illustrates how meeting PCI DSS requirements may help entities demonstrate how NIST Framework outcomes are achieved for payment environments.

Stakeholders can use this mapping to identify opportunities for control efficiencies and greater alignment between organizational security objectives. For example, the mapping can help identify where the implementation of a particular security control can support both a PCI DSS requirement and a NIST Framework outcome. Additionally, an entity's internal evaluations to determine the effectiveness of implemented controls may help the entity prepare for either a PCI DSS or NIST Framework assessment, or both. In this way, the mapping supports a consistent and coordinated approach to information security across an organization.

The mapping is not a tool for demonstrating compliance to either PCI DSS or the NIST Framework, nor does meeting either a PCI DSS requirement or its corresponding NIST Framework outcome result in the other being met.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
FUNCTION: IDENTIFY (ID)		
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried.	• **CIS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8, PM-5 • **PCI DSS v3.2.1** 2.4, 9.9, 11.1.1, 12.3.3
	ID.AM-2: Software platforms and applications within the organization are inventoried.	• **CIS CSC** 2 • **COBIT 5** BAI09.01, BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 • **NIST SP 800-53 Rev. 4** CM-8, PM-5 • **PCI DSS v3.2.1** 2.4, 12.3.7

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
	ID.AM-3: Organizational communication and data flows are mapped.	• **CIS CSC** 12 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8, A.13.2.2 • **PCI DSS v3.2.1** 1.1.2, 1.1.3
	ID.AM-4: External information systems are catalogued.	• **CIS CSC** 12 • **COBIT 5** APO02.02, APO10.04, DSS01.02 • **ISO/IEC 27001:2013** A.11.2.6 • **NIST SP 800-53 Rev. 4** AC-20, SA-9 • **PCI DSS v3.2.1** 1.1.1, 1.1.2, 1.1.3, 2.4
	ID.AM-5: Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value.	• **CIS CSC** 13, 14 • **COBIT 5** APO03.03, APO03.04, AP012.01, BA104.02, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.6 • **ISO/IEC 27001:2013** A.8.2.1 • **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6 • **PCI DSS v3.2.1** 9.6.1, 12.2
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.	• **CIS CSC** 117, 19 • **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1 • **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11 • **PCI DSS v3.2.1** 12.4, 12.5, 12.8, 12.9

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated.	• **COBIT 5** APO08.01, AP008.04, APO08.05, APO10.03, APO10.04, APO10.05 • **ISO/IEC 27001:2013** A.15.1.1, A.15.1.12, A-15.1.3, A.15.2.1, A.15.2.2 • **NIST SP 800-53 Rev. 4** CP-2, SA-12
	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated.	• **COBIT 5** APO02.06, APO03.01 • **ISO/IEC** 27001:2013 Clause 4.1 • **NIST SP 800-53 Rev. 4** PM-8
	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated.	• **COBIT 5** APO02.01, APO02.06, APO03.01 • **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 • **NIST SP 800-53 Rev. 4** PM-11, SA-14
	ID.BE-4: Dependencies and critical functions for delivery of critical services are established.	• **COBIT** 5 APO10.01, BAI04.02, BAI09.02 • **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 • **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
	ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations).	• **OBIT 5** BAI03.02, DSS04.02 • **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 • **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-13, SA-14

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational cybersecurity policy is established and communicated.	• **CIS CSC** 19 • **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02 • **ISA 62443-2-1:2009** 4.3.2.6 • **ISO/IEC 27001:2013** A.5.1.1 • **NIST SP 800-53 Rev. 4** -1 controls from all families • **PCI DSS v3.2.1** 1.5, 2.5, 3.7, 4.3, 5.4, 6.7, 7.3, 8.8, 9.10, 10.8, 11.6, 12.1
	ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.	• **CIS CSC** 19 • **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1 • **NIST SP 800-53 Rev. 4** PM-1, PM-2, PS-7 • **PCI DSS v3.2.1** 12.4, 12.5, 12.8, 12.9
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.	• **CIS CSC** 19 • **COBIT 5** BJI02.01, MEA03.01, MEA03.04 • **ISA 62443-2-1:2009** 4.4.3.7 • **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 • **NIST SP 800-53 Rev. 4** -1 controls from all security control families • **PCI DSS v3.2.1** 3.1, 12.10
	ID.GV-4: Governance and risk management processes address cybersecurity risks.	• **COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02 • **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 • **ISO/IEC 27001:2013** Clause 6 • **NIST SP 800-53 Rev. 4** SA-2, PM-3, PM-7, PM-9, PM-10, PM-11 • **PCI DSS v3.2.1** 1.5, 2.5, 3.7, 4.3, 5.4, 6.7, 7.3, 8.8, 9.10, 10.8, 11.6, 12.1, 12.2

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented.	• **CIS CSC** 4 • **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 • **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 • **PCI DSS v3.2.1** 6.1, 11.2, 11.3, 12.2
	ID.RA-2: Cyber threat intelligence and vulnerability information is received from information sharing forums and sources.	• **CIS CSC** 4 • **COBIT 5** BAI08.01 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 • **ISO/IEC 27001:2013** A.6.1.4 • **NIST SP 800-53 Rev. 4** PM-15, PM-16, SI-5 • **PCI DSS v3.2.1** 6.1
	ID.RA-3: Threats, both internal and external, are identified and documented.	• **CIS CSC** 4 • **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 • **ISO/IEC** 27001:2013 Clause 6.1.2 • **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16 • **PCI DSS v3.2.1** 12.2

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
	ID.RA-4: Potential business impacts and likelihoods are identified.	• **CIS CSC** 4 • **COBIT 5** DSS04.02 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 • **ISO/IEC** 27001:2013 A.16.1.6, Clause 6.1.2 • **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-9, PM-11, SA-14 • **PCI DSS v3.2.1** 6.1
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	• **CIS CSC** 4 • **COBIT 5** APO12.02 • **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16 • **PCI DSS v3.2.1** 12.2
	ID.RA-6: Risk responses are identified and prioritized.	• **CIS CSC** 4 • **COBIT 5** APO12.05, APO13.02 • **ISO/IEC 27001:2013** Clause 6.1.3 • **NIST SP 800-53 Rev. 4** PM-4, PM-9 • **PCI DSS v3.2.1** 12.10.1

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	• **CIS CSC** 4 • **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 • **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3, Clause 9.3 • **ISA 62443-2-1:2009** 4.3.4.2 • **NIST SP 800-53 Rev. 4** PM-9 • **PCI DSS v3.2.1** 12.2
	ID.RM-2: Organizational risk tolerance is determined and clearly expressed	• **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.3.2.6.5 • **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 • **NIST SP 800-53 Rev. 4** PM-9 • **PCI DSS v3.2.1** 12.2
	ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	• **COBIT 5** APO12.06 • **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 • **NIST SP 800-53 Rev. 4** PM-8, PM-9, PM-11, SA-14 • **PCI DSS v3.2.1** 12.2

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	• **CIS CSC:** 4.8 • **COBIT 5:** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 • **ISA 62443-2-1:2009**: 4.3.4.2 • **ISO/IEC 27001:2013:** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1,A.15.2.2 • **NIST SP 800-53:** SA-9, SA-12, PM-9 • **PCI DSS v3.2.1** 12.2, 12.8, 12.9
	ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	• **COBIT 5:** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 • **ISA 62443-2-1:2009:** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6,4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 • **ISO/IEC 27001:2013:** A.15.2.1, A.15.2.2 • **NIST SP 800-53**: RA-2, RA-3, SA-12, SA-14, SA-15, PM-9 • **PCI DSS v3.2.1** 12.2, 12.8
	ID.SC-3: Contracts with suppliers and third- party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity and Cyber Supply Chain Risk Management Plan.	• **COBIT 5:** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 • **ISA 62443-2-1:2009:** 4.3.2.6.4, 4.3.2.6.7 • **ISO/IEC 27001:2013:** A.15.1.1, A.15.1.2, A.15.1.3 • **NIST SP 800-53:** SA-9, SA-11, SA-12, PM-9 • **PCI DSS v3.2.1** 12.8, 12.9

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
	ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm that they are meeting their contractual obligations.	• **COBIT 5:** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 • **ISA 62443-2-1:2009:** 4.3.2.6.7 • **ISA 62443-3-3:2013:** SR 6.1 • **ISO/IEC 27001:2013:** A.15.2.1, A.15.2.2 • **NIST SP 800-53**: AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12 • **PCI DSS v3.2.1** 12.8
	ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers.	• **CIS CSC:** 19, 20 • **COBIT 5:** DSS04.04 • **ISA 62443-2-1:2009:** 4.3.2.5.7, 4.3.4.5.11 • **ISA 62443-3-3:2013:** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 • **ISO/IEC 27001:2013** A.17.1.3 • **NIST SP 800-53**: CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9 • **PCI DSS v3.2.1** 12.10
FUNCTION: PROTECT (PR)		
Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	• **CIS CSC** 1.5, 15, 16 • **COBIT 5** DSS05.04, DSS06.03 • **ISA 62443-2-1:2009** 4.3.3.5.1 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 • **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 • **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11 • **PCI DSS v3.2.1** 2.1, 8.1, 8.2, 8.5, 8.6, 12.3

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
	PR.AC-2: Physical access to assets is managed and protected.	• **COBIT 5** DSS01.04, DSS05.05 • **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 • **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.3 1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 • **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8 • **PCI DSS v3.2.1** 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.9, 9.10
	PR.AC-3: Remote access is managed.	• **CIS CSC** 12 • **COBIT 5** APO13.01, DSS01.04, DSS05.03 • **ISA 62443-2-1:2009** 4.3.3.6.6 • **ISA 62443-3-3:2013** SR 1.13, SR 2.6 • **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-1, AC-17, AC-19, AC-20 • **PCI DSS v3.2.1** 2.3, 8.1.5, 8.3, 8.5.1, 12.3.8, 12.3.9, 12.3.10
	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	• **CIS CSC 3, 5,** 12, 14, 15, 16, 18 • **COBIT 5** DSS05.04 • **ISA 62443-2-1:2009** 4.3.3.7.3 • **ISA 62443-3-3:2013** SR 2.1 • **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 • **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24 • **PCI DSS v3.2.1** 6.4.2, 7.1, 7.2, 8.7, 9.3

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
	PR.AC-5: Network integrity is protected (e.g. network segregations, network segmentation).	• **CIS CSC** 9, 14, 15, 18 • **COBIT 5** DSS01.05, DSS05.02 • **ISA 62443-2-1:2009** 4.3.3.4 • **ISA 62443-3-3:2013** SR 3.1, SR 3.8 • **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 • **NIST SP 800-53 Rev. 4** AC-4, AC-10, SC-7 • **PCI DSS v3.2.1** 1.1, 1.2, 1.3, 2.2, 6.2, 10.8, 11.3
	PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.	• **CIS CSC 16** • **COBIT 5:** DSS05.04, DSS05.05, DSS05.07, DSS06.03 • **ISA 62443-2-1:2009:** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 • **ISA 62443-3-3:2013:** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.9, SR 2.1 • **ISO/IEC 27001:2013:** A.7.1.1, A.9.1.2 • **NIST SP 800-53: Rev 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3 • **PCI DSS v3.2.1** 7.1.4, 8.1, 8.2.2

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).	• **CIS CSC** 1, 12, 15, 16 • **COBIT 5:** DSS05.04, DSS05.10, DSS06.10 • **ISA 62443-2-1:2009:** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4,4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 • **ISA 62443-3-3:2013:** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9,SR 1.10 ISO/IEC 27001:2013 A.9.2.1, • **ISO/IEC 27001:2013: A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3,A.18.1.4** • **NIST SP 800-53: Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14,IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11 • **PCI DSS v3.2.1** 8.2, 8.3
Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained.	• **CIS CSC** 17, 18 • **COBIT 5** APO07.03, BAI05.07 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 • **NIST SP 800-53 Rev. 4** AT-2, PM-13 • **PCI DSS v3.2.1** 6.7, 7.3, 8.4, 9.9.3, 12.4, 12.6
	PR.AT-2: Privileged users understand their roles and responsibilities.	• **CIS CSC** 5, 17, 18 • **COBIT 5** APO07.02, DSS05.04, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 • **NIST SP 800-53 Rev. 4** AT-3, PM-13 • **PCI DSS v3.2.1** 1.1.5, 7.1, 7.2, 7.3, 12.4, 12.6

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.	• **CIS CSC** 17 • **COBIT 5** APO07.03, APO07.06, APO10.04, APO10.05 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2 • **NIST SP 800-53 Rev. 4** PS-7, SA-9, SA-16 • **PCI DSS v3.2.1** 12.8.2, 12.9
	PR.AT-4: Senior executives understand their roles and responsibilities.	• **CIS CSC** 17, 19 • **COBIT 5** EDM01.01, APO01.02, APO07.03 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, • **NIST SP 800-53 Rev. 4** AT-3, PM-13 • **PCI DSS v3.2.1** 12.4, 12.5
	PR.AT-5: Physical cybersecurity security personnel understand their roles and responsibilities.	• **CIS CSC** 17 • **COBIT 5** APO07.03 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, • **NIST SP 800-53 Rev. 4** AT-3, IR-2, PM-13 • **PCI DSS v3.2.1** 12.4, 12.5

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected.	• **CIS CSC** 13, 14 • **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 • **ISA 62443-3-3:2013** SR 3.4, SR 4.1 • **ISO/IEC 27001:2013** A.8.2.3 • **NIST SP 800-53 Rev. 4** MP-8, SC-12, SC-28 • **PCI DSS v3.2.1** 3 (all), 8.2.1
	PR.DS-2: Data-in-transit is protected.	• **CIS CSC** 13, 14 • **COBIT 5** APO01.06, DSS05.02, DSS06.06 • **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 • **NIST SP 800-53 Rev. 4** SC-8, SC-11, SC-12 • **PCI DSS v3.2.1** 4 (all), 8.2.1
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition.	• **CIS CSC** 1 • **COBIT 5** BAI09.03 • **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.4.4.1 • **ISA 62443-3-3:2013** SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 • **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16 • **PCI DSS v3.2.1** 2.4, 9.5, 9.6, 9.7, 9.8, 9.9
	PR.DS-4: Adequate capacity to ensure availability is maintained.	• **CIS CSC** 1, 2, 13 • **COBIT 5** APO13.01, BAI04.04 • **ISA 62443-3-3:2013** SR 7.1, SR 7.2 • **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1 • **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
	PR.DS-5: Protections against data leaks are implemented.	• **CIS CSC** 13 • **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02 • **ISA 62443-3-3:2013** SR 5.2 • **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 • **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 • **PCI DSS v3.2.1** 10.6
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	• **CIS CSC** 2.3 • **COBIT 5** APO01.06, BAI06.01, DSS06.02 • **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 • **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 • **NIST SP 800-53 Rev. 4** SC-16, SI-7 • **PCI DSS v3.2.1** 11.5
	PR.DS-7: The development and testing environment(s) are separate from the production environment.	• **CIS CSC** 18, 20 • **COBIT 5** BAI03.08, BAI07.04 • **ISO/IEC 27001:**2013 A.12.1.4 • **NIST SP 800-53 Rev. 4** CM-2 • **PCI DSS v3.2.1** 6.4.1, 6.4.2

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
	PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity.	• **COBIT 5:** BAI03.05 • **ISA 62443-2-1:2009:** 4.3.4.4.4 • **ISO/IEC 27001:2013: A.11.2.4** • **NIST SP 800-53: SA-10, SI-7** • **PCI DSS v3.2.1** 9.9.2
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).	• **CIS CSC** 3, 9, 11 • **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 • **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 • **ISA 62443-3-3:2013** SR 7.6 • **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10 • **PCI DSS v3.2.1** 1.2, 2.2
	PR.IP-2: A System Development Life Cycle to manage systems is implemented.	• **CIS CSC** 18 • **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03 • **ISA 62443-2-1:2009** 4.3.4.3.3 • **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 • **NIST SP 800-53 Rev. 4** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17 • **PCI DSS v3.2.1** 6.3, 6.4, 6.5, 6.6, 6.7

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
	PR.IP-3: Configuration change control processes are in place.	• **CIS CSC** 3, 11 • **COBIT 5** BAI01.06, BAI06.01, • **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 • **ISA 62443-3-3:2013** SR 7.6 • **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10 • **PCI DSS v3.2.1** 6.4
	PR.IP-4: Backups of information are conducted, maintained, and tested periodically.	• **CIS CSC** 10 • **COBIT 5** APO13.01, DSS01.01, DSS04.07 • **ISA 62443-2-1:2009** 4.3.4.3.9 • **ISA 62443-3-3:2013** SR 7.3, SR 7.4 • **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 • **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9 • **PCI DSS v3.2.1** 9.5.1, 12.10.1, 12.10.2
	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met.	• **COBIT 5** DSS01.04, DSS05.05 • **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 • **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 • **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18 • **PCI DSS v3.2.1** 9 (all)

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
	PR.IP-6: Data is destroyed according to policy.	• **COBIT 5** BAI09.03, DSS05.06 • **ISA 62443-2-1:2009** 4.3.4.4.4 • **ISA 62443-3-3:2013** SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 • **NIST SP 800-53 Rev. 4** MP-6 • **PCI DSS v3.2.1** 3.1, 9.8
	PR.IP-7: Protection processes are improved.	• **COBIT 5** APO11.06, APO12.06, DSS04.05 • **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5,4.4.3.6, 4.4.3.7, 4.4.3.8 • **ISO/IEC 27001:2013** A.16.1.6, Clause 9, Clause 10 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6 • **PCI DSS v3.2.1** 10.8, 12.10.6, 12.11
	PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties.	• **COBIT 5** BAI08.04, DSS03.04 • **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	• **CIS CSC** 19 • **COBIT 5** APO12.06, DSS04.03 • **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 • **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 • **NIST SP 800-53 Rev. 4** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17 • **PCI DSS v3.2.1** 11.1.2, 12.5.3, 12.10

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
	PR.IP-10: Response and recovery plans are tested.	• **CIS CSC** 19, 20 • **COBIT 5** DSS04.04 • **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 • **ISA 62443-3-3:2013** SR 3.3 • **ISO/IEC 27001:2013** A.17.1.3 • **NIST SP 800-53 Rev. 4** CP-4, IR-3, PM-14 • **PCI DSS v3.2.1** 12.10.2
	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).	• **CIS CSC** 5, 16 • **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 • **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 • **ISO/IEC 27001:2013** A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.7.3.1, A.8.1.4 • **NIST SP 800-53 Rev. 4** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21 • **PCI DSS v3.2.1** 8.1.3, 9.3, 12.7
	PR.IP-12: A vulnerability management plan is developed and implemented.	• **CIS CSC** 4, 18, 20 • **COBIT 5** BAI03.10, DSS05.01, DSS05.02 • **ISO/IEC 27001:2013** A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 • **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2 • **PCI DSS v3.2.1** 6.1, 6.2, 6.5, 11.2

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.	• **COBIT 5** BAI03.10, BAI09.02, BAI09.0, DSS01.05 • **ISA 62443-2-1:2009** 4.3.3.3.7 • **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 • **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5, MA-6 • **PCI DSS v3.2.1** 6.2, 9.9.3
	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	• **CIS CSC** 3, 5 • **COBIT 5** DSS05.04 • **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 • **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 • **NIST SP 800-53 Rev. 4** MA-4 • **PCI DSS v3.2.1** 8.1.5, 8.3, 8.5.1, 12.3.8, 12.3.9
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	• **CIS CSC** 1, 3, 5, 6, 14, 15, 16 • **COBIT 5** APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 • **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 • **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 • **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 • **NIST SP 800-53 Rev. 4** AU Family • **PCI DSS v3.2.1** 10.1, 10.2, 10.3, 10.4, 10.5, 10.6.1, 10.6.2, 10.7
	PR.PT-2: Removable media is protected and its use restricted according to policy.	• **CIS CSC** 8, 13 • **COBIT 5** APO13.01, DSS05.02, DSS05.06 • **ISA 62443-3-3:2013** SR 2.3 • **ISO/IEC 27001:2013** A.8.2.1, A.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 • **NIST SP 800-53 Rev. 4** MP-2, MP-3, MP-4, MP-5, MP-7, MP-8 • **PCI DSS v3.2.1** 3.4, 9.5, 9.6, 9.7, 9.8, 12.3, 12.3.10

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
	PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	• **CIS CSC** 3, 11, 14 • **COBIT 5** DSS05.02, DSS05.05, DSS06.06 • **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 • **ISO/IEC 27001:2013** A.9.1.2 • **NIST SP 800-53 Rev. 4** AC-3, CM-7 • **PCI DSS v3.2.1** 2.2, 7.1, 7.2, 9.3
	PR.PT-4: Communications and control networks are protected.	• **CIS CSC** 8, 12, 15 • **COBIT 5** DSS05.02, APO13.01 • **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 • **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3 • **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43 • **PCI DSS v3.2.1** 1 (all), 2 (all)
	PR.PT-5: Systems operate in pre-defined functional states to achieve availability (e.g. under duress, under attack, during recovery, normal operations).	• **COBIT 5:** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 • **ISA 62443-2-1:2009:** 4.3.2.5.2 • **ISA 62443-3-3:2013: SR 7.1, SR 7.2 ISO/IEC** • **27001:2013: A.17.1.2, A.17.2.1** • **NIST SP 800-53: CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6**

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
FUNCTION: DETECT (DE)		
Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed.	• **CIS CSC** 1, 4, 6, 12, 13, 15, 16 • **COBIT 5** DSS03.01 • **ISA 62443-2-1:2009** 4.4.3.3 • **ISO/IEC 27001:2013: A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2** • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4 • **PCI DSS v3.2.1** 1.1.1, 1.1.2, 1.1.3
	DE.AE-2: Detected events are analyzed to understand attack targets and methods.	• **CIS CSC** 3, 6, 13, 15 • **COBIT 5** DSS05.07 • **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 • **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4 • **PCI DSS v3.2.1** 10.6 (all), 12.5.2
	DE.AE-3: Event data are collected and correlated from multiple sources and sensors.	• **CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 • **COBIT 5** BAI08.02 • **ISA 62443-3-3:2013** SR 6.1 • **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4 • **PCI DSS v3.2.1** 10.1, 12.10.5, 10.6

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
	DE.AE-4: Impact of events is determined.	• **CIS CSC** 4, 6 • **COBIT 5** APO12.06, DSS03.01 • **ISO/IEC 27001:2013** A.16.1.4 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI -4 • **PCI DSS v3.2.1** 10.6.3, 12.5.2
	DE.AE-5: Incident alert thresholds are established.	• **CIS CSC** 6, 19 • **COBIT 5** APO12.06, DSS03.01 • **ISA 62443-2-1:2009** 4.2.3.10 • **ISO/IEC 27001:2013** A.16.1.4 • **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8 • **PCI DSS v3.2.1** 12.5.2
Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events.	• **CIS CSC** 7, 8, 12, 13, 15, 16 • **COBIT 5 DSS01.03, DSS03.05,** DSS05.07 • **ISA 62443-3-3:2013** SR 6.2 • **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4 • **PCI DSS v3.2.1** 10.6.1, 10.6.2, 11.4
	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.	• **COBIT 5** DSS01.04, DSS01.05 • **ISA 62443-2-1:2009** 4.3.3.3.8 • **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2 • **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20 • **PCI DSS v3.2.1** 9.1.1

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	• **CIS CSC** 5, 7, 14, 16 • **COBIT 5** DSS05.07 • **ISA 62443-3-3:2013** SR 6.2 • **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3 • **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11 • **PCI DSS v3.2.1** 9.1.1
	DE.CM-4: Malicious code is detected.	• **CIS CSC** 4, 7, 8, 12 • **COBIT 5** DSS05.01 • **ISA 62443-2-1:2009** 4.3.4.3.8 • **ISA 62443-3-3:2013** SR 3.2 • **ISO/IEC 27001:2013** A.12.2.1 • **NIST SP 800-53 Rev. 4** SI-3, SI-8 • **PCI DSS v3.2.1** 5 (all)
	DE.CM-5: Unauthorized mobile code is detected.	• **CIS CSC** 7, 8 • **COBIT 5** DSS05.01 • **ISA 62443-3-3:2013** SR 2.4 • **ISO/IEC 27001:2013** A.12.5.1, A-12.6.2 • **NIST SP 800-53 Rev. 4** SC-18, SI-4. SC-44 • **PCI DSS v3.2.1** 5 (all)
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.	• **COBIT 5** APO07.06, APO10.05 • **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 • **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4 • **PCI DSS v3.2.1** 8.1.5, 10.6

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	• **CIS CSC** 1, 2, 3, 5, 9, 12, 13, 15, 16 • **COBIT 5** DSS05.02, DSS05.05 • **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1 • **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4 • **PCI DSS v3.2.1** 10.1, 10.6.1, 11.1, 11.4, 11.5, 12.10.5
	DE.CM-8: Vulnerability scans are performed.	• **CIS CSC** 4, 20 • **COBIT 5** BAI03.10, DSS05.01 • **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 • **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Rev. 4** RA-5 • **PCI DSS v3.2.1** 11.2
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability.	• **CIS CSC** 19 • **COBIT 5** APO01.02, DSS05.01, DSS06.03 • **ISA 62443-2-1:2009** 4.4.3.1 • **ISO/IEC 27001:2013** A.6.1.1 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14 • **PCI DSS v3.2.1** 9.9.3, 12.5.2, 12.10
	DE.DP-2: Detection activities comply with all applicable requirements.	• **COBIT 5** DSS06.01, MEA03.03, MEA03.04 • **ISA 62443-2-1:2009** 4.4.3.2 • **ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A-18.2.3 • **NIST SP 800-53 Rev. 4** AC-25, CA-2, CA-7, PM-14, SA-18, SI-4 • **PCI DSS v3.2.1** 10.9, 11.2, 11.3, 11.4, 12.10.1

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
	DE.DP-3: Detection processes are tested.	• **COBIT 5** APO13.02, DSS05.02 • **ISA 62443-2-1:2009** 4.4.3.2 • **ISA 62443-3-3:2013** SR 3.3 • **ISO/IEC 27001:2013** A.14.2.8, A.7.2.2 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, PM-14, SI-3, SI-4 • **PCI DSS v3.2.1** 10.6.1, 10.9, 11.2, 11.3, 12.10
	DE.DP-4: Event detection information is communicated.	• **CIS CSC** 19 • **COBIT 5** APO08.04, APO12.06, DSS02.05 • **ISA 62443-2-1:2009** 4.3.4.5.9 • **ISA 62443-3-3:2013** SR 6.1 • **ISO/IEC 27001:2013** A.16.1.2, A-16.1.3 • **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4 • **PCI DSS v3.2.1** 12.10
	DE.DP-5: Detection processes are continuously improved.	• **COBIT 5** APO11.06, APO12.06, DSS04.05 • **ISA 62443-2-1:2009** 4.4.3.4 • **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14 • **PCI DSS v3.2.1** 12.10.6

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
FUNCTION: RESPOND (RS)		
Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents	**RS.RP-1:** Response plan is executed during or after an incident.	• **CIS CSC** 19 • **COBIT 5** APO12.06, BAI01.10 • **ISA 62443-2-1:2009** 4.3.4.5.1 • **ISO/IEC 27001:2013** A.16.1.5 • **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8 • **PCI DSS v3.2.1** 12.10
Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies)	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed.	• **CIS CSC** 19 • **COBIT 5** EDM03.02, APO01.02, APO12.03 • **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 • **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8 • **PCI DSS v3.2** 12.10
	RS.CO-2: Incidents are reported consistent with established criteria.	• **CIS CSC** 19 • **COBIT 5** DSS01.03 • **ISA 62443-2-1:2009** 4.3.4.5.5 • **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 • **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8 • **PCI DSS v3.2.1** 10.8, 12.10DD

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
	RS.CO-3: Information is shared consistent with response plans.	• **CIS CSC** 19 • **COBIT 5** DSS03.04 • **ISA 62443-2-1:2009** 4.3.4.5.2 • **ISO/IEC 27001:2013** A.16.1.2, Clause 7.4, Clause 16.1.2 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4 • **PCI DSS v3.2.1** 12.10
	RS.CO-4: Coordination with stakeholders occurs consistent with response plans.	• **CIS CSC** 19 • **COBIT 5** BAI08.04 • **ISA 62443-2-1:2009** 4.3.4.5.5 • **ISO/IEC 27001:2013** Clause 7.4 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 • **PCI DSS v3.2.1** 12.10.1
	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.	• **CIS CSC** 19 • **COBIT 5** BAI08.04 • **ISO/IEC 27001:2013** A.6.1.4 • **NIST SP 800-53 Rev. 4** PM-15, SI-5
Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated.	• **CIS CSC** 4, 6, 8, 19 • **COBIT 5** DSS02.04, DSS02.07 • **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • **ISA 62443-3-3:2013** SR 6.1 • **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4 • **PCI DSS v3.2.1** 10.6.3, 11.5.1, 12.5.2, 12.10.5

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
	RS.AN-2: The impact of the incident is understood.	• **COBIT 5** DSS02.02 • **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 • **NIST SP 800-53 Rev. 4** CP-2, IR-4 • **PCI DSS v3.2.1** 10.6.3, 11.5.1, 12.5.2
	RS.AN-3: Forensics are performed.	• **COBIT 5** APO12.06, DSS03.02, DSS05.07 • **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR3.9, SR 6.1 • **ISO/IEC 27001:2013** A.16.1.7 • **NIST SP 800-53 Rev. 4** AU-7, IR-4 • **PCI DSS v3.2.1** 11.5.1, 12.5.2
	RS.AN-4: Incidents are categorized consistent with response plans.	• **CIS CSC** 4, 19 • **COBIT 5** DSS02.02 • **ISA 62443-2-1:2009** 4.3.4.5.6 • **ISO/IEC 27001:2013** A.16.1.4 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8 • **PCI DSS v3.2.1** 11.5.1, 12.5.2
	RS.AN-5: Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers).	• **CIS CSC** 4, 19 • **COBIT 5** EDM03.02, DSS05.07 • **NIST 800-53 Rev 4** SI-5, PM-15 • **PCI DSS v3.2.1** 6.1, 6.2

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	**RS.MI-1:** Incidents are contained.	• **CIS CSC** 19 • **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.3.4.5.6 • **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 • **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 • **NIST SP 800-53 Rev. 4** IR-4 • **PCI DSS v3.2.1** 11.5.1, 12.5.2
	RS.MI-2: Incidents are mitigated.	• **CIS CSC** 4, 19 • **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 • **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 • **NIST SP 800-53 Rev. 4** IR-4 • **PCI DSS v3.2.1** 11.5.1, 12.5.2
	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.	• **CIS CSC** 4 • **COBIT 5** APO12.06 • **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5 • **PCI DSS v3.2.1** 6.1, 6.2, 10.6.3, 11.2, 11.5.1, 12.5.2, 12.10
Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and	**RS.IM-1:** Response plans incorporate lessons learned.	• **COBIT 5** BAI01.13 • **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 • **ISO/IEC 27001:2013** A.16.1.6, Clause 10 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 • **PCI DSS v3.2.1** 12.10.6

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
previous detection/response activities.	**RS.IM-2:** Response strategies are updated.	• **COBIT 5** BAI01.13, DSS04.08 • **ISO/IEC 27001:2013** A.16.1.6, Clause 10 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 • **PCI DSS v3.2.1**12.10.6
FUNCTION: RECOVER (RC)		
Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity incidents.	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident.	• **CIS CSC** 10 • **COBIT 5** APO12.06, DSS02.05, DSS03.04 • **ISO/IEC 27001:2013** A.16.1.5 • **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8 • **PCI DSS v3.2.1** 12.10.6
Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned.	• **COBIT 5** APO12.06, BAI05.07, DSS04.08 • **ISA 62443-2-1:2009** 4.4.3.4 • **ISO/IEC 27001:2013** A.16.1.6, Clause 10 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 • **PCI DSS v3.2.1** 12.10.6
	RC.IM-2: Recovery strategies are updated.	• **COBIT 5** APO12.06, BAI07.08 • **ISO/IEC 27001:2013** A.16.1.6, Clause 10 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 • **PCI DSS v3.2.1** 12.10.6

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	**RC.CO-1:** Public relations are managed.	• **COBIT 5** EDM03.02 • **ISO/IEC 27001:2013** A.6.1.4, Clause 7.4
	RC.CO-2: Reputation is repaired after an incident.	• **COBIT 5** MEA03.02 • **ISO/IEC 27001:2013** Clause 7.4
	RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.	• **COBIT 5** APO12.06 • **ISO/IEC 27001:2013** Clause 7.4 • **NIST SP 800-53 Rev. 4** CP-2, IR-4

16 Appendix E: NIST Privacy Framework

Version 1.0

IT SECURITY PLAN TEMPLATE

Certain Categories or Subcategories may be identical to or have been adapted from the Cybersecurity Framework. The following legend can be used to identify this relationship in the table. A complete crosswalk between the two frameworks can be found in the resource repository at https://www.nist.gov/privacy-framework.

The Function, Category, or Subcategory aligns with the Cybersecurity Framework, but the text has been adapted for the Privacy Framework.

The Category or Subcategory is identical to the Cybersecurity Framework.

	Function	Category	Subcategory
	IDENTIFY-P (ID-P): Develop the organizational understanding to manage privacy risk for individuals arising from data processing.	**Inventory and Mapping (ID.IM-P):** Data processing by systems, products, or services is understood and informs the management of privacy risk.	**ID.IM-P1:** Systems/products/services that process data are inventoried.
			ID.IM-P2: Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried.
			ID.IM-P3: Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried.
			ID.IM-P4: Data actions of the systems/products/services are inventoried.
			ID.IM-P5: The purposes for the data actions are inventoried.
			ID.IM-P6: Data elements within the data actions are inventoried.
			ID.IM-P7: The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).
			ID.IM-P8: Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services.

Function	Category	Subcategory
	Business Environment (ID.BE-P): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform privacy roles, responsibilities, and risk management decisions.	**ID.BE-P1:** The organization's role(s) in the data processing ecosystem are identified and communicated.
		ID.BE-P2: Priorities for organizational mission, objectives, and activities are established and communicated.
		ID.BE-P3: Systems/products/services that support organizational priorities are identified and key requirements communicated.
	Risk Assessment (ID.RA-P): The organization understands the privacy risks to individuals and how such privacy risks may create follow-on impacts on organizational operations, including mission, functions, other risk management priorities (e.g., compliance, financial), reputation, workforce, and culture.	**ID.RA-P1:** Contextual factors related to the systems/products/services and the data actions are identified (e.g., individuals' demographics and privacy interests or perceptions, data sensitivity and/or types, visibility of data processing to individuals and third parties).
		ID.RA-P2: Data analytic inputs and outputs are identified and evaluated for bias.
		ID.RA-P3: Potential problematic data actions and associated problems are identified.
		ID.RA-P4: Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.
		ID.RA-P5: Risk responses are identified, prioritized, and implemented.
	Data Processing Ecosystem Risk Management (ID.DE-P): The organization's priorities, constraints, risk tolerance, and assumptions are established and used to support risk decisions associated with managing privacy risk and third parties within the data processing ecosystem. The organization has established and implemented the processes to identify, assess, and manage privacy risks within the data processing ecosystem.	**ID.DE-P1:** Data processing ecosystem risk management policies, processes, and procedures are identified, established, assessed, managed, and agreed to by organizational stakeholders.
		ID.DE-P2: Data processing ecosystem parties (e.g., service providers, customers, partners, product manufacturers, application developers) are identified, prioritized, and assessed using a privacy risk assessment process.
		ID.DE-P3: Contracts with data processing ecosystem parties are used to implement appropriate measures designed to meet the objectives of an organization's privacy program.
		ID.DE-P4: Interoperability frameworks or similar multi-party approaches are used to manage data processing ecosystem privacy risks.

	Function	Category	Subcategory
			ID.DE-P5: Data processing ecosystem parties are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual, interoperability framework, or other obligations.
	GOVERN-P (GV-P): Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.	**Governance Policies, Processes, and Procedures (GV.PO-P):** The policies, processes, and procedures to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk.	**GV.PO-P1:** Organizational privacy values and policies (e.g., conditions on data processing such as data uses or retention periods, individuals' prerogatives with respect to data processing) are established and communicated.
			GV.PO-P2: Processes to instill organizational privacy values within system/product/service development and operations are established and in place.
			GV.PO-P3: Roles and responsibilities for the workforce are established with respect to privacy.
			GV.PO-P4: Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners).
			GV.PO-P5: Legal, regulatory, and contractual requirements regarding privacy are understood and managed.
			GV.PO-P6: Governance and risk management policies, processes, and procedures address privacy risks.
		Risk Management Strategy (GV.RM-P): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**GV.RM-P1:** Risk management processes are established, managed, and agreed to by organizational stakeholders.
			GV.RM-P2: Organizational risk tolerance is determined and clearly expressed.
			GV.RM-P3: The organization's determination of risk tolerance is informed by its role(s) in the data processing ecosystem.
		Awareness and Training (GV.AT-P): The organization's workforce and third parties engaged in data processing are provided privacy awareness education and are trained to perform their privacy-related duties and responsibilities consistent with	**GV.AT-P1:** The workforce is informed and trained on its roles and responsibilities.
			GV.AT-P2: Senior executives understand their roles and responsibilities.
			GV.AT-P3: Privacy personnel understand their roles and responsibilities.

	Function	Category	Subcategory
		related policies, processes, procedures, and agreements and organizational privacy values.	**GV.AT-P4:** Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities.
		Monitoring and Review (GV.MT-P): The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.	**GV.MT-P1:** Privacy risk is re-evaluated on an ongoing basis and as key factors, including the organization's business environment (e.g., introduction of new technologies), governance (e.g., legal obligations, risk tolerance), data processing, and systems/products/services change.
			GV.MT-P2: Privacy values, policies, and training are reviewed and any updates are communicated.
			GV.MT-P3: Policies, processes, and procedures for assessing compliance with legal requirements and privacy policies are established and in place.
			GV.MT-P4: Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place.
			GV.MT-P5: Policies, processes, and procedures are established and in place to receive, analyze, and respond to problematic data actions disclosed to the organization from internal and external sources (e.g., internal discovery, privacy researchers, professional events).
			GV.MT-P6: Policies, processes, and procedures incorporate lessons learned from problematic data actions.
			GV.MT-P7: Policies, processes, and procedures for receiving, tracking, and responding to complaints, concerns, and questions from individuals about organizational privacy practices are established and in place.
	CONTROL-P (CT-P): Develop and implement appropriate activities to enable organizations or individuals to manage data with	**Data Processing Policies, Processes, and Procedures (CT.PO-P):** Policies, processes, and procedures are maintained and used to manage data processing (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) consistent with the	**CT.PO-P1:** Policies, processes, and procedures for authorizing data processing (e.g., organizational decisions, individual consent), revoking authorizations, and maintaining authorizations are established and in place.
			CT.PO-P2: Policies, processes, and procedures for enabling data review, transfer, sharing or disclosure, alteration, and deletion are established and in place (e.g., to maintain data quality, manage data retention).

	Function	Category	Subcategory
	sufficient granularity to manage privacy risks.	organization's risk strategy to protect individuals' privacy.	**CT.PO-P3:** Policies, processes, and procedures for enabling individuals' data processing preferences and requests are established and in place.
			CT.PO-P4: A data life cycle to manage data is aligned and implemented with the system development life cycle to manage systems.
		Data Processing Management (CT.DM-P): Data are managed consistent with the organization's risk strategy to protect individuals' privacy, increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization).	**CT.DM-P1:** Data elements can be accessed for review.
			CT.DM-P2: Data elements can be accessed for transmission or disclosure.
			CT.DM-P3: Data elements can be accessed for alteration.
			CT.DM-P4: Data elements can be accessed for deletion.
			CT.DM-P5: Data are destroyed according to policy.
			CT.DM-P6: Data are transmitted using standardized formats.
			CT.DM-P7: Mechanisms for transmitting processing permissions and related data values with data elements are established and in place.
			CT.DM-P8: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.
			CT.DM-P9: Technical measures implemented to manage data processing are tested and assessed.
			CT.DM-P10: Stakeholder privacy preferences are included in algorithmic design objectives and outputs are evaluated against these preferences.
		Disassociated Processing (CT.DP-P): Data processing solutions increase disassociability consistent with the organization's risk strategy to protect individuals' privacy and enable implementation of privacy principles (e.g., data minimization).	**CT.DP-P1:** Data are processed to limit observability and linkability (e.g., data actions take place on local devices, privacy-preserving cryptography).
			CT.DP-P2: Data are processed to limit the identification of individuals (e.g., de-identification privacy techniques, tokenization).
			CT.DP-P3: Data are processed to limit the formulation of inferences about individuals' behavior or activities (e.g., data processing is decentralized, distributed architectures).
			CT.DP-P4: System or device configurations permit selective collection or disclosure of data elements.
			CT.DP-P5: Attribute references are substituted for attribute values.

	Function	Category	Subcategory
	COMMUNICATE-P (CM-P): Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks.	**Communication Policies, Processes, and Procedures (CM.PO-P):** Policies, processes, and procedures are maintained and used to increase transparency of the organization's data processing practices (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) and associated privacy risks.	**CM.PO-P1:** Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established and in place.
			CM.PO-P2: Roles and responsibilities (e.g., public relations) for communicating data processing purposes, practices, and associated privacy risks are established.
		Data Processing Awareness (CM.AW-P): Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mechanisms are used and maintained to increase predictability consistent with the organization's risk strategy to protect individuals' privacy.	**CM.AW-P1:** Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place.
			CM.AW-P2: Mechanisms for obtaining feedback from individuals (e.g., surveys or focus groups) about data processing and associated privacy risks are established and in place.
			CM.AW-P3: System/product/service design enables data processing visibility.
			CM.AW-P4: Records of data disclosures and sharing are maintained and can be accessed for review or transmission/disclosure.
			CM.AW-P5: Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources) in the data processing ecosystem.
			CM.AW-P6: Data provenance and lineage are maintained and can be accessed for review or transmission/disclosure.
			CM.AW-P7: Impacted individuals and organizations are notified about a privacy breach or event.
			CM.AW-P8: Individuals are provided with mitigation mechanisms (e.g., credit monitoring, consent withdrawal, data alteration or deletion) to address impacts of problematic data actions.
	PROTECT-P (PR-P): Develop and implement	**Data Protection Policies, Processes, and Procedures (PR.PO-P):** Security and privacy policies (e.g., purpose, scope, roles	**PR.PO-P1:** A baseline configuration of information technology is created and maintained incorporating security principles (e.g., concept of least functionality).

Function	Category	Subcategory
appropriate data processing safeguards.	and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data.	**PR.PO-P2:** Configuration change control processes are established and in place.
		PR.PO-P3: Backups of information are conducted, maintained, and tested.
		PR.PO-P4: Policy and regulations regarding the physical operating environment for organizational assets are met.
		PR.PO-P5: Protection processes are improved.
		PR.PO-P6: Effectiveness of protection technologies is shared.
		PR.PO-P7: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed.
		PR.PO-P8: Response and recovery plans are tested.
		PR.PO-P9: Privacy procedures are included in human resources practices (e.g., deprovisioning, personnel screening).
		PR.PO-P10: A vulnerability management plan is developed and implemented.
	Identity Management, Authentication, and Access Control (PR.AC-P): Access to data and devices is limited to authorized individuals, processes, and devices, and is managed consistent with the assessed risk of unauthorized access.	**PR.AC-P1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.
		PR.AC-P2: Physical access to data and devices is managed.
		PR.AC-P3: Remote access is managed.
		PR.AC-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.
		PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).
		PR.AC-P6: Individuals and devices are proofed and bound to credentials, and authenticated commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).
	Data Security (PR.DS-P): Data are managed consistent with the	**PR.DS-P1:** Data-at-rest are protected.
		PR.DS-P2: Data-in-transit are protected.

Function	Category	Subcategory
	organization's risk strategy to protect individuals' privacy and maintain data confidentiality, integrity, and availability.	**PR.DS-P3:** Systems/products/services and associated data are formally managed throughout removal, transfers, and disposition.
		PR.DS-P4: Adequate capacity to ensure availability is maintained.
		PR.DS-P5: Protections against data leaks are implemented.
		PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.
		PR.DS-P7: The development and testing environment(s) are separate from the production environment.
		PR.DS-P8: Integrity checking mechanisms are used to verify hardware integrity.
	Maintenance (PR.MA-P): System maintenance and repairs are performed consistent with policies, processes, and procedures.	**PR.MA-P1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.
		PR.MA-P2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.
	Protective Technology (PR.PT-P): Technical security solutions are managed to ensure the security and resilience of systems/products/services and associated data, consistent with related policies, processes, procedures, and agreements.	**PR.PT-P1:** Removable media is protected and its use restricted according to policy.
		PR.PT-P2: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
		PR.PT-P3: Communications and control networks are protected.
		PR.PT-P4: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situation.

17 Appendix F: Glossary

Common Terms	Definitions
Accreditation	The official management decision given by a senior SO official to authorize operation of an information system and to explicitly accept the risk to SO operations (including mission, functions, image, or reputation), SO assets, or individuals, based on the implementation of an agreed-upon set of security controls.
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.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authorizing Official	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to SO operations (including mission, functions, image, or reputation), SO assets, or individuals.
Availability	Ensuring timely and reliable access to and use of information.
Common Security Control	Security control that can be applied to one or more SO information systems and has the following properties: (i) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (ii) the results from the assessment of the control can be used to support the security certification and accreditation processes of an SO information system where that control has been applied.
Compensating Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST SP 800-53, that provide equivalent or comparable protection for an information system.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Configuration Control	Process for controlling modifications to hardware, firmware, software, and documentation to ensure that the information system is protected against improper modifications before, during, and after system implementation.
High Impact System	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high.

Information Owner	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Security Policy	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information System Owner	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
Information System Security Officer	Individual assigned responsibility by the senior information security officer, authorizing official, management official, or information system owner for ensuring that the appropriate operational security posture is maintained for an information system or program.
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Low Impact System	An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low.
Major Application	An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.
Major Information System	An information system that requires special management attention because of its importance to an SO mission; its high development, operating, or maintenance costs; or its significant role in the administration of SO programs, finances, property, or other resources.
Management Controls	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
Mobile Code	Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.

Moderate Impact System	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high.
Operational Controls	The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Remote Access	Access by users (or information systems) communicating external to an information system security perimeter.
Remote Maintenance	Access by users (or information systems) communicating external to an information system security perimeter.
Risk	The level of impact on SO operations (including mission, functions, image, or reputation), SO assets, or individuals results from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
Risk Assessment	The process of identifying risks to SO operations (including mission, functions, image, or reputation), SO assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.
Risk Management	The process of managing risks to SO operations (including mission, functions, image, or reputation), SO assets, or individuals resulting from the operation of an information system. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.
Safeguards	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
Security Boundary	The defined set of systems that are under a single administrative control. These boundaries occur at various levels, and vulnerabilities can become apparent as data “crosses” each one. These enclaves subdivide an organization’s information system into security groupings with common risk profiles and mitigation methodologies.

Security Category	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.
Security Control Baseline	The set of minimum security controls defined for a low impact, moderate-impact, or high-impact information system.
Security Requirements	Requirements levied on an information system that are derived from laws, executive orders, directives, policies, instructions, regulations, or organizational (mission) needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
System Security Plan	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
Technical Controls	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
User	Individual or (system) process authorized to access an information system.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Vulnerability Assessment	Formal description and evaluation of the vulnerabilities in an information system.

18 Appendix G: Acronyms and Abbreviations

Acronym	Definition
AC	Access Control
ACID	Atomicity, Consistency, Isolation, Durability
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
BFS	Bureau of the Fiscal Service
BIA	Business Impact Analysis

BoE	Board of Education
C3	CISCO Command Center
CAB	Change Advisory Board
CAP	Corrective Action Plan
CERT	Computer Emergency Readiness Team
CFO	Chief Financial Officer
CI&A	Confidentiality, Integrity, and Availability
CIPA	Children's Internet Protection Act
CIPM	Critical Infrastructure Protection Manager
CIS	Critical Information Security
CISO	Chief Information Security Officer
CITR	Commerce Interim Technical Requirement
CM	Configuration Management
CMP	Configuration Management Plan
CMS	Centers for Medicare and Medicaid Services
CNSS	Committee on National Security Systems
CO	Contracting Officer
COO	Chief Operating Officer
COOP	Continuity of Operations
COPPA	Children's Online Privacy Protection Act
COTR	Contracting Officer's Technical Representative
CP	Contingency Plan or Planning
CPIC	Capital Planning and Investment Control
CTO	Chief Technology Officer
DATO	Denial of Authorization to Operate
DHCP	Dynamic Host Configuration Protocol
DI	Directory Information
DISA	Defense Information Systems Agency
DLA	Data Loss Prevention
DM	Data Minimization and Retention
DNS	Domain Name System
DoIT	Department of Information Technology
DOO	Department Organization Order
DRP	Disaster Recovery Plan
DTI	Department of Technology Infrastructure
EA	Enterprise Architecture
EPMS	Enterprise Program Management System
EPO	Emergency Power Off
ESEA	Elementary and Secondary Education Act of 1965
ESSA	Every Student Succeeds Act
FAFSA	Federal Acquisition Streamlining Act of 1994
FERPA	Family Educational Rights and Privacy Act
FCG	Frederick County Government

FCPS	Frederick County Public Schools
FFMIA	Federal Financial Management Improvement Act
FIPS	Federal Information Processing Standards
FISCAM	Federal Information Systems Controls Audit Manual
FISMA 2004	Federal Information Security Management Act of 2002
FISMA 2014	Federal Information Security Modernization Act of 2014
FTI	Federal Tax Information
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
GLBA	Gramm-Leach-Bliley Act
GPEA	Government Paperwork Elimination Act
GPRA	Government Performance and Results Act
GSA	General Services Administration
GUI	Graphical User Interface
HIPPA	Health Insurance Portability and Accountability Act of 1996
HSPD	Homeland Security Presidential Directive
IA	Identification and Authentication
IaaS	Infrastructure as a Service
IDEA	Individuals with Disabilities Education Act
IDS	Intrusion Detection Systems
IEO	Office of Infrastructure Engineering and Operations
IMAP	Internet Message Access Protocol
INFOSEC	Information Systems Security
IATT	Interim Authority to Test
IP	Individual Participation and Redress
IR	Incident Response
IS	Information System
IRS	Internal Revenue Service
IRT	Incident Response Team
IS2P2	Information Systems Security and Privacy Policy
ISA	Interconnection Security Agreement
ISO	Information System Owner
ISSM	Information Systems Security Manager
ISSO	Information System Security Officer
IT	Information Technology
LAN	Local Area Network
LDI	Limited Directory Information
LEA	Local Education Agency
MA	Maintenance
MIS	Maryland Information System

MOU/A	Memorandum of Understanding/Agreement
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
OCSE	Federal Office of Child Support Enforcement
OCISO	Office of the Chief Information Officer
OGC	Office of General Counsel
OIG or AG	Office of Inspector General
OIMS	Office of Information Management Services
OLA	Office of Legislative Audits
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
PaaS	Platform as a Service
PE	Physical and Environmental Protection
PCI	Payment Card Information
PCI-DSS	Payment Card Industry – Data Security Standard
PCI SSC	Payment Card Industry Security Standards Council
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PII-A	Personally Identifiable Information - Adult
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PL	Planning
PM	Project Manager
PO	Privacy Officer
POA&M	Plan of Action and Milestones
POC	Point of Contact
POP	Post Office Protocol
PRA	Preliminary Risk Assessment
PS	Personnel Security
PTA	Privacy Threshold Analysis
RA	Risk Assessment
RAR	Risk Assessment Report
RBAC	Role Based Access Control
RFC	Request for Comment
RM	Records Management
RoB	Rules of Behavior

RPC	Remote Procedure Call
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SA	System and Services Acquisition
SaaS	Software as a Service
SANS	SysAdmin, Audit, Network and Security Institute
SAD	System Architecture Documentation
SAP	Security Assessment Plan
SAR	Security Assessment Report
SC	Security Category
SDLC	System Development Life Cycle
SE	Security
SecCat	Security Categorization
SI	System and Information Integrity
SIA	Security Impact Assessment
SLA	Service Level Agreement
SO	System Owner
SOP	Standard Operating Procedure
SORN	Systems of Records Notices
SP	Special Publication
SPII	Student Personally Identifiable Information
SSA	Social Security Administration
SSH	Secure Shell
SSO	Single Sign-On
SSP	System Security Plan
STIG	Security Technical Implementation Guide
ST&A	Security Test and Assessment
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
TIGTA	Treasury Inspector General for Tax Administration
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
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WISP	Written Information Security Program