Department of Commerce

Enterprise Cybersecurity Policy (ECP)

Office of Cybersecurity and
IT Risk Management (OCRM)

Office of the Chief Information Officer (OCIO)

September 2022

Version 1.1

Contents

1 Introduction

1.1 Background

The Department of Commerce's (Department or DOC) mission is to foster the conditions for economic growth and opportunity for all communities. The DOC's mission impacts industry, Federal agencies, local, tribal, state, and international governments, and the American people in many ways. Accordingly, the work on behalf of these constituents is either directly or indirectly reliant on DOC information and information systems to foster, promote, and develop the foreign and domestic commerce of the United States (U.S.).

It is vital that the information systems which collect, process, transmit, store, and disseminate DOC information implement the necessary safeguards and best practices to protect the confidentiality, integrity, and availability of its information and assets in accordance with the Federal Information Security Modernization Act of 2014 (FISMA), and Office of Management and Budget Circular A-130 (OMB A-130), *Managing Information as a Strategic Resource.* To meet these requirements, the Office of Cybersecurity and IT Risk Management (OCRM) develops and maintains the Department's Enterprise Cybersecurity Policy (ECP) which defines the requirements for managing an enterprise-wide Cybersecurity Program (Cybersecurity Program) for the Department.

1.2 Purpose

The ECP establishes the Cybersecurity Program governance framework, and roles and responsibilities for implementing security and privacy controls throughout the Department. The OCRM performs annual reviews of the ECP and will make updates as necessary to ensure alignment with new Federal policy, mandates, standards, and guidance issued by the OMB, National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), Committee on National Security Systems (CNSS), Office of the National Cyber Director (ONCD), and the Office of the Director of National Intelligence (ODNI). All DOC Bureaus must adhere to the ECP and may develop supplemental policy if necessary to address specific Bureau mission needs. However, Bureau supplemental policy must meet or exceed the minimum requirements set forth in the ECP.

1.3 Scope and Applicability

The ECP applies to all DOC information and information systems (unclassified and classified) that collect, process, transmit, store, and disseminate DOC information including contractor-managed, cloud services, and systems leveraged from other Federal agencies. Bureaus must hold Federal employees, contractors, guest researchers, collaborators, and individuals with access to the Department's information and information systems and assets accountable for adhering to the ECP.

The DOC monitors and manages cybersecurity-related risks through the implementation of the NIST Federal Information Processing Standards Publication 200 (FIPS 200), *Minimum Security Requirements for Federal Information and Information Systems*, and appropriate DOC risk

mitigation strategies. In addition, DOC classified information systems must adhere to the CNSS,[1] and Intelligence Community (IC) policy and directives, as applicable.

1.4 Authorities and Applicable Federal Mandates

Reference Appendix A.

1.5 Effective Date

The ECP is effective upon final approval and issuance. Bureaus must adhere to and implement the ECP requirements and update Bureau specific policies and procedures as applicable. Bureaus requesting to waive requirements established in the ECP must follow the OCRM waiver request process. All requests must be submitted by the Bureau Chief Information Officer (CIO) to the DOC Chief Information Security Officer (CISO) for review and recommendation to the DOC CIO.

1.6 Order of Precedence and Succession

This policy replaces the DOC Information Technology Security Baseline Policy (ITSBP), Version 1.0, June 24, 2019, but leaves in place the topical security requirements captured in the ITSBP annex series C and D. The C and D annexes will remain in effect until superseded by forthcoming Standards and Handbooks. Each forthcoming Standard and Handbook will identify the ITSBP annex it cancels. Upon release of all applicable Standards and Handbooks, full cancellation of the ITSBP and its annexes will be announced by the DOC OCIO.

Additionally, while the C and D annexes of the ITSBP remain in effect, to the extent that any of their provisions conflict with provisions of this policy, this policy will control.

[1] CNSSI 1253, *Security Categorization and Control Selection for National Security Systems.*

2 Policy

In accordance with FISMA and OMB A-130, the Department maintains a Cybersecurity Program that facilitates the protection of DOC information, information systems, and operations. The OCRM establishes the governance framework, policy requirements, and standards for managing the security of DOC's Information Technology (IT).[2]

While cybersecurity and privacy are independent disciplines, both are closely related, therefore it is essential for the Department to take a coordinated approach in identifying and managing risks. The DOC CISO provides oversight on DOC's Cybersecurity Program while the Senior Agency Official for Privacy (SAOP), in coordination with OCRM, serves as the central authority for privacy within DOC.

2.1 Serve as the Central Focal Point for Cybersecurity

The OCRM serves as the central focal point and enforces enterprise-wide cybersecurity management while providing oversight on the implementation of Federal cybersecurity requirements. To strengthen the Department's cybersecurity posture, OCRM and Bureaus must continue collaborating to support the unique missions and business functions necessary to meet requirements set forth by Federal mandates and Departmental authorities referenced in Appendix A.

2.2 Implement an Enterprise Cybersecurity Program

The DOC Cybersecurity Program defines goals for and delegates cybersecurity responsibilities to the Bureaus. These goals represent baseline expectations for DOC's cybersecurity posture, taking into consideration the respective business needs and missions of each Bureau. The adoption of a DOC Common Controls Program (CCP) and enterprise security architecture will result in more efficient and effective implementation of security requirements.

2.3 Institute a Cybersecurity Governance Framework

The DOC cybersecurity governance framework serves as the foundation for the Cybersecurity Program. The ECP, Security and Privacy Control Matrix (SPCM), Standards, and Handbooks collectively provide flexibility for the Cybersecurity Program to adapt to evolving threats and effectively manage risks. This framework publishes:

- **Policy** as the primary mechanism to enforce cybersecurity requirements and define roles and responsibilities.
- **SPCM** to supplement policy by identifying organizationally defined control parameters, in accordance with NIST SP 800-53.[3]

[2] Any service, equipment, or interconnected system(s) or subsystem(s) in use to support the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. https://csrc.nist.gov/glossary/term/information_technology.

[3] NIST SP 800-53 Rev.5, *Security and Privacy Controls for Information Systems and Organizations.*

- **Standards** based on the SPCM with specific technical requirements for Cybersecurity Program areas.
- **Handbooks** to guide the implementation of processes in support of the policy, and SPCM.

2.4 Promote Awareness of Cybersecurity Risks

Cybersecurity awareness and training is a vital program and DOC information system users must be continually educated on cybersecurity and privacy risks which may jeopardize the Department's critical mission. The OCRM will continue collaborating with Bureaus to highlight these risks while promoting cybersecurity awareness and training.

2.5 Manage an Effective Cybersecurity Program

The management of DOC information and information systems must be implemented to ensure effectiveness based on a thorough examination of the risks identified in security assessments and the impact the information system has on DOC operations, assets, and individuals. Additionally, the Cybersecurity Program must be continually evaluated to ensure it addresses emerging threats to DOC information and information systems and to inform DOC's Enterprise Risk Management (ERM) Program.

The concepts found within FISMA, OMB A-130, NIST Risk Management Framework (RMF), Cybersecurity Framework (CSF), and NIST Special Publication (SP) 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, comprise the basis for DOC's Cybersecurity Program. The Cybersecurity Program provides a formal, structured approach for developing risk assessments for information systems and provides a uniform standard for evaluating security risks to information systems operating by or on behalf of DOC. The primary focus of this approach must be on the information system's mission, not on the specific IT resource. The effective management of risks is essential to protecting the information and information systems that enable the Department's critical mission.

2.6 Require the Use of the Department's System of Record

The Cyber Security Assessment and Management (CSAM)[4] application is the Department's formal system of record for all FISMA-reportable information systems inventory and security assessment and authorization management. CSAM is an enterprise solution and provides a holistic view of cybersecurity risk management activities across the Department, including RMF and CSF implementation and delivers reporting capabilities necessary to meet FISMA requirements.

All Bureaus requesting DOC CIO authorization for the use of alternate tools other than CSAM to perform RMF and CSF activities must:

- Work with OCRM to establish automated feeds to ingest information to perform the required quality control, validation, and oversight on Bureau security assessment and

[4] CSAM is authorized by the DHS Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Quality Services Management Office (Cyber QSMO) as a service to reduce the time and cost involved in sourcing and maintaining an enterprise-wide risk assessment platform. Reference https://www.cisa.gov/qsmo-services-risk-assessment.

privacy control implementation. At a minimum, Bureaus must provide the System Security and Privacy Plan (SSPP), Security Assessment Plan (SAP), Risk Assessment Results (RAR), Security Assessment Report (SAR), and Plan of Action and Milestones (POA&M) attributes into CSAM; and

- Follow the OCRM policy waiver process which requires the Bureau CIO[5] submit a request to the DOC CISO who will review and provide a formal recommendation to the DOC CIO.

2.7 Promote Emerging Security Technologies

The Department must embrace a forward-leaning enterprise security architecture which entails transitioning away from legacy systems and adopting modern and emerging technologies. This includes, but is not limited to, accelerating the use of secure cloud services, migrating to a Zero Trust Architecture (ZTA), implementing strong multifactor authentication (MFA) and encryption; and increasing mobile threat defenses.[6] Bureaus must collaborate with OCRM to reduce the Department's legacy IT footprint, evaluate emerging technologies, and assess opportunities for integration to achieve enterprise solutions whenever possible.

2.8 Implement Secure Cloud Services

A key element to accelerating secure cloud adoption requires the successful implementation of security and privacy controls, continuous monitoring, risk management, and oversight of cloud services. Bureaus that use cloud services must adhere to and hold Cloud Service Providers (CSPs) accountable for meeting the requirements established in this ECP. All cloud services leveraged by DOC must meet the Federal Risk and Authorization Management Program (FedRAMP) requirements, implement the CSP provided customer responsibility matrix, and complete the DOC RMF processes to obtain authority to operate (ATO).

2.9 Strengthening the Supply Chain

The Department's Supply Chain Risk Management (SCRM) Program, managed under OCRM, oversees supply chain risks by implementing requirements of the law, Federal mandates, and NIST guidance. In accordance with Section 514 of the Consolidated Appropriations Act of 2022,[7] as amended and as may be subsequently updated in future Appropriations Act provisions, the Department is required to conduct an assessment of the risk of cyber-espionage or sabotage associated with the acquisition of a new FIPS 199 high impact or moderate impact information system.[8] Prior to the Bureau acquisition of any such system, the Department must determine that the acquisition is in the interest of the Department and U.S. Bureaus, Offerors, and Awardees must

[5] All waiver requests must be submitted within the first quarter per fiscal year, no later than December 31, and approved waivers must be renewed annually.

[6] Consistent with Executive Order 14028 *Improving the Nations Cybersecurity,* DOC must reduce reliance on legacy systems, leverage emerging technologies to increase cyber resiliency and defenses against evolving threats.

[7] H.R.2471 - Consolidated Appropriations Act, 2022.

[8] A new procurement is associated with a high or moderate impact system as defined by the security categorization process in accordance with FIPS 199, subject to the reporting requirements of 44 U.S.C. Section 3505, and for which either: (1) a new system inventory record will be entered in CSAM; or (2) an existing inventory record will be modified in CSAM.

adhere to the Department's SCRM Program requirements and processes and provide information to the Department's SCRM Program necessary to make an informed risk-based decision.

3 Roles and Responsibilities

3.1 DOC Chief Information Officer

In accordance with the Department Organizational Order (DOO) 15-23, *Chief Information Officer,* the DOC CIO will:

i. Report to the Secretary of Commerce and OMB on the status of the DOC's Enterprise Cybersecurity Program;

ii. Carry out responsibilities under the Federal Information Technology Acquisition Reform Act (FITARA);

iii. Appoint a CISO to carry out the Cybersecurity Program as required by FISMA;

iv. Ensure that Bureau Officials provide cybersecurity protections commensurate with the potential risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of:

   a. information collected or maintained by or on behalf of DOC; and

   b. information systems used or operated by an agency, a contractor of an agency, or another organization on behalf of an agency;

v. Enforce DOC's enterprise-wide Cybersecurity Policies, including levying sanctions on Bureaus for non-compliance;

vi. Coordinate the evaluations of new and emerging technologies and maintain a central repository;

vii. Ensure cybersecurity management processes are integrated with DOC and/or Bureau strategic and operational planning processes;

viii. Approve or deny Bureau-level requests to waive enterprise-wide Cybersecurity Policy requirements based upon recommendations from the DOC CISO;

ix. Approve the use of encryption technologies that are not FIPS 140-2 or higher validated in those situations where FIPS-validated products are not available; and

x. Develop, implement, and manage an enterprise-wide POA&M process to correct cybersecurity weaknesses.

The DOC CIO may delegate any cybersecurity-related responsibilities listed above to the DOC CISO with the exception of responsibility ix.

3.2 DOC Chief Information Security Officer

The DOC CISO is the Senior Agency Information Security Officer (SAISO) who is responsible for the management and oversight of the DOC Cybersecurity Program and its associated functions, including those delegated by the DOC CIO. The CISO serves as the principal lead to implement FISMA and OMB A-130 requirements throughout the Department. These functions are inherently

governmental and therefore must be assigned to U.S. Government personnel only. The DOC CISO will:

i. Develop and maintain a Cybersecurity Program;

ii. Provide leadership to both the CIO Council and CISO Council and guide the management and implementation of DOC's Cybersecurity Program;

iii. Develop policy, standards, and handbooks for implementing FISMA and OMB A-130 security requirements;

iv. Develop, implement, and maintain an enterprise-wide Cybersecurity Policy Framework for related security and privacy controls to cost-effectively reduce risks to an acceptable level;

v. Maintain Bureau oversight on security and privacy assessment and authorization activities to include monitoring, evaluating, and ensuring periodic testing of controls and techniques to validate that they are effectively implemented;

vi. Establish, implement, assess, and manage the Department's common security controls program;

vii. Enforce and monitor the implementation of a comprehensive cybersecurity awareness and training program, which includes simulations and exercises to assist DOC's workforce with making informed cybersecurity decisions;

viii. Review and recommend approval or denial to the DOC CIO of Bureau-level requests to waive enterprise-wide Cybersecurity Policy requirements;

ix. Prepare and submit the quarterly DOC CIO FISMA metrics and annual FISMA report to OMB and DHS CISA;

x. Provide oversight on all cybersecurity related audits, investigations, and engagements from the Government Accountability Office (GAO) and Office of Inspector General (OIG); and

xi. Serve as the DOC CIO's liaison to external Federal agencies for all matters related to the implementation of DOC's Cybersecurity Program.

3.3 Head of Bureau

The Head of Bureau or designee(s) must establish and maintain a Bureau-wide cybersecurity program in accordance with the DOC ECP, SPCM, Standards, and Handbooks. The Head of Bureau or designee(s) are ultimately responsible for implementing Bureau level security protections commensurate with the potential risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of Bureau information systems. The Head of Bureau or designee(s) works with the DOC CISO through the DOC CISO Council to carry out the following Bureau level responsibilities:

i. Implement the requirements established via the enterprise-wide Cybersecurity Program and documents listed above;

ii. Implement security and privacy assessment and authorization activities to include tracking and reporting on the Bureaus' FISMA-reportable information system inventory to verify:

(1) assessment planning procedures are documented prior to the execution of an assessment; (2) system security documentation is accurate;

iii. Develop, implement, manage, and prioritize closure of POA&Ms (including cybersecurity-related GAO and OIG findings);

iv. Integrate security in the Capital Planning and Investment Control (CPIC) process;

v. Assign a Bureau representative to work with OCRM in support of DOC's annual and ad-hoc cybersecurity audits, investigation, and engagements;

vi. Collaborate with OCRM to evaluate emerging technologies, assess opportunities for integration, and securely adopt additional cloud services to achieve enterprise solutions whenever possible; and

vii. Document, review, test, and update Information System Contingency Plans (ISCP), Incident Response Plans (IRP), and implement lessons learned.

4 Information System Security and Privacy Requirements

The DOC Cybersecurity Program is continuously evaluated to ensure its policies, standards, and handbooks align with FISMA and OMB A-130 requirements. Incorporating the use of automation whenever possible[9], all Bureaus must implement and manage security and privacy control requirements to avoid, detect, counteract, and minimize security risks to physical property, information, information systems, and privacy of information or other assets.

4.1 Security and Privacy Control Families

Security and privacy controls are designed to be technology agnostic allowing the focus to be on the fundamental countermeasures needed to protect DOC information and information systems. The following subsections define the general-security and privacy control requirements for all DOC systems.

For the detailed minimum-security requirements for DOC information systems, reference the SPCM, Standards, and Handbooks.

4.1.1 Access Control

Bureaus must implement account management and apply access controls on every information system and must:

i. Protect DOC information systems, data, and assets from unauthorized access, alteration, loss, unavailability, or disclosure of information;

ii. Limit access to non-public DOC information systems to authorized users, processes acting on behalf of authorized users, or devices (including other information systems);

iii. Restrict remote access to non-public DOC information systems to authorized devices using FIPS validated or National Security Agency (NSA) approved encryption, unless otherwise approved by the DOC CIO;

iv. Control and manage emergency and temporary access authorizations, and require approval from an account authorizer before access is granted; and

v. Apply usage restrictions, configuration/connection requirements, and guidance for each type of remote access allowed.

4.1.2 Awareness and Training

Users with access to DOC information systems and data must complete annual cybersecurity and privacy awareness training, and any additional training requirement necessary at the Department and Bureau level. Bureaus must track and maintain compliance to:

i. Ensure users of DOC information systems are aware of the security risks associated with their activities, laws, regulations, directives, policies, standards, and procedures related to the security of DOC information systems and data (digital and printed);

[9] https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

ii. Provide personnel with role-based training to carry out their assigned information system security-related duties and responsibilities; and

iii. Maintain records of information security and privacy training completion and include security awareness training on recognizing and reporting potential indicators of insider threat.

4.1.3 Audit and Accountability

Bureau information systems must enable audit logging, and monitoring solutions necessary to support incident response, audit log analysis, and log correlation. To support these requirements, Bureaus must:

i. Enable, protect, and retain information system audit records to facilitate security monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity;

ii. Ensure users are held accountable for the activities performed on the information systems; and

iii. Provide all relevant security monitoring, auditing data, and security incident-related data to the Enterprise Security Operations Center (ESOC) in accordance with the DOC ECP, SPCM, Standards, and Handbooks.

4.1.4 Assessment, Authorization, and Monitoring

Bureaus must complete security and privacy assessment and authorization activities in accordance with the DOC ECP, SPCM, Standards, and Handbooks. Prior to operations, all information systems must obtain an ATO. Utilizing CSAM,[10] Bureaus must:

i. Document information system security and privacy control implementation in a SSPP;

ii. Implement security and privacy controls;

iii. Document a comprehensive SAP;

iv. Execute assessments in accordance with the SAP;

v. Produce a RAR and SAR to determine if security and privacy controls are effective;

vi. Develop, monitor, and implement POA&Ms to correct deficiencies to reduce or eliminate vulnerabilities;

vii. Authorize the operation of DOC information systems and any associated information system interconnections prior to operational use; and

viii. Perform Information Security Continuous Monitoring (ISCM), assessing the DOC Core Controls on operational systems to determine continued effectiveness in providing an appropriate level of protection.

[10] Reference Section 2.6 of the DOC ECP, *Requires the Use of the Department's System of Record*.

4.1.5 Configuration Management

Bureaus must develop and implement configuration management to assess and authorize information system changes. To support these requirements, Bureaus must:

i. Establish and maintain baseline configurations and inventories of DOC information systems (including hardware, software, firmware, and documentation) throughout the respective System Development Lifecycle (SDLC);

ii. Establish a configuration change control process which includes a security impact assessment to ensure proposed changes are properly evaluated, tested, approved, and documented before being put into production;

iii. Establish and enforce security settings consistent with the information system operational requirements and validate those controls through DOC-approved tools; and

iv. Limit access to only authorized personnel to make information system changes.

4.1.6 Contingency Planning

Contingency planning is necessary to support an information system's availability, recovery, and reconstitution during a contingency event. Bureaus must:

i. Document a comprehensive ISCP to include a Business Impact Analysis (BIA);

ii. Coordinate ISCP training and testing with related plans such as Disaster Recovery Plans (DRP), Continuity of Operations Plans (COOP), and IRP to assess the readiness to execute the plan; and

iii. Establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for DOC information systems to ensure the availability of critical IT resources and continuity of operations in emergency situations.

4.1.7 Identification and Authentication

Bureaus must implement secure identification and authentication processes on all DOC information systems. In accordance with the Homeland Security Presidential Directive 12 (HSPD-12) compliant credentials, including but not limited to Personal Identity Verification Credential (PIV), Personal Identity Verification Interoperable Credential (PIV-I), and Derived PIV where applicable in accordance with Federal requirements. DOC allows the use of PIV and other forms of approved MFA solutions as the primary means of identification and authentication to DOC information systems, Federally controlled facilities, and other secure areas by Federal employees and contractors. Bureaus must:

i. Identify information system users, processes acting on behalf of users, and/or devices; and

ii. Authenticate (or verify) the identities of information system users, processes, and/or devices prior to authorizing access to DOC information systems and data (this does not apply to unauthenticated access to public information).

4.1.8 Incident Response

The ESOC is the central authority for the Department's incident handling, response, reporting, and management for security and privacy. In support of these functions, Bureaus are responsible for providing security monitoring, auditing data, and security incident-related data to the ESOC. Bureaus must:

i. Establish an operational incident handling capability that includes adequate preparation, detection and analysis, containment, eradication and recovery, post-incident activities, and user response activities in coordination with the ESOC;

ii. Track, document, and report security incidents to the ESOC;

iii. Follow the CISA's Cybersecurity Incident Response playbook for cybersecurity incidents in cooperation with DOC ESOC for incident handling;

iv. Support the ESOC by providing digital forensic and other information necessary to support security incident investigation upon request; and

v. Provide training to employees and contractors on incident reporting and response activities.

4.1.9 Maintenance

In conjunction with the Bureaus configuration management procedures, information system maintenance must be controlled, authorized, and monitored accordingly. Bureaus must:

i. Create information system maintenance processes to demonstrate periodic and timely maintenance on DOC information systems;

ii. Implement effective controls on the tools, techniques, mechanisms, and personnel used to conduct on-site and remote information system maintenance;

iii. Restrict non-local system maintenance and diagnostics to authorized privileged personnel; and

iv. Disable maintenance ports during normal system operation and ensure they are only enabled during approved maintenance activities.

4.1.10 Media Protection

Bureaus must document and implement a media protection process to demonstrate protection of information system media in all forms. Bureaus must:

i. Mark, protect, store, process, and transmit DOC data relative to the sensitivity classification;

ii. Limit the use of file sharing to only authorized solutions;

iii. Encrypt information on all removable media;

iv. Sanitize information system media per NIST Special Publication 800-88[11] before release for reuse or destroy the media if no longer in use; and

v. Ensure all IT equipment is sanitized in accordance with media protection requirements before being removed from a Bureau's physical control.

4.1.11 Physical and Environmental Protection

Bureau information systems hosted on-premises must implement physical and environmental security controls at the hosting facility. Bureaus must:

i. Plan physical controls and processes in conjunction with information systems, equipment, and the respective operating environments;

ii. Limit physical access to information systems, equipment, and the respective operating environments to authorized individuals;

iii. Monitor and log physical access to the facility;

iv. Implement security controls to prevent accidental damage, disruption, and physical tampering to transmission and distribution lines;

v. Protect power equipment and cabling from damage and destruction;

vi. Implement sufficient emergency power and lighting so that they remain available in the event of an information system or facility failure;

vii. Employ and maintain sufficient fire detection and suppression systems at the facility; and

viii. Protect the information system from water damage by providing master shutoff or isolation valves that are accessible and working properly.

4.1.12 Planning

The SSPP is critical to ensuring security and privacy controls that are planned or in place are adequately documented. Bureaus must:

i. Create, document, review, and update annually (at minimum) an SSPP in CSAM;

ii. Develop security and privacy architectures for the information system that describe the requirements and approach to protect the confidentiality, integrity, and availability of the information system; and

iii. Provide and maintain Rules of Behavior (ROB) for all individuals who access the information system.

4.1.13 Program Management

The Program Management (PM) controls are essential for establishing minimum security and privacy requirements necessary to support the Department's Cybersecurity Program. To reduce the burden on Bureau assessment and authorization activities, where appropriate OCRM will

[11] NIST SP 800-88 Rev.1, *Guidelines for Media Sanitization*.

coordinate with responsible entities to implement, assess, and manage and offer for inheritance, applicable PM controls as a DOC CCP.

4.1.14 Personnel Security

Access to DOC information systems must be limited to only authorized personnel supporting the development, operation, management, or maintenance of information systems, including providing information system support. Bureaus must:

i. Ensure individuals that occupy positions of responsibility within the Bureau (including third-party service providers) are assigned risk designations, and meet security criteria established by DOC's Office of Security (OSY) for those positions;

ii. Protect DOC information and information systems during and after personnel actions such as termination and transfer; and

iii. Employ formal sanctions for personnel failing to comply with DOC personnel security policy and procedures, consistent with DOC personnel security policy.

4.1.15 Personally Identifiable Information Processing and Transparency

In coordination with the Office of Privacy and Open Government (OPOG), Bureaus must complete a Privacy Threshold Assessment (PTA), Privacy Impact Assessment (PIA), and System of Record Notice (SORN), as applicable for information systems that collect, use, store, and/or transmit Personally Identifiable Information (PII), in accordance with OMB M-03-22.[12]

4.1.16 Risk Assessment

Bureau information systems must have a documented risk assessment in accordance with the DOC ECP, SPCM, Standards, and Handbooks. The risk assessment must be consistent with the security categorization of the information system and impact to the confidentiality, integrity, and availability of the data the information system stores, processes, and transmits. Bureaus must:

i. Perform automated vulnerability and secure configuration scans using DOC-approved tools;

ii. Perform penetration testing on applicable information systems;

iii. Analyze, monitor, remediate, and report on information system vulnerabilities; and

iv. Periodically assess the risk to Bureau information systems.

4.1.17 System and Services Acquisition

The procurement of tools, technologies, and services must adhere to the DOC Procurement Policy, which takes into consideration the impact to the DOC mission. Bureaus must:

i. Demonstrate a business justification for the procurement along with allocation of sufficient resources to protect DOC information and information systems;

[12] Reference Attachment D located in M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.*

ii. Employ SDLC processes that incorporate information system security considerations;

iii. Ensure new acquisitions of technology include available security configurations;

iv. Perform supply chain risk assessments and ensure supply chain risk management processes are in place for IT acquisitions, as required by Procurement Memorandum 2015-08;[13]

v. Implement software usage and installation restrictions on DOC information systems and comply with applicable copyright laws and licensing agreements;

vi. Hold third-party providers contractually accountable to comply with the DOC ECP, SPCM Standards, and Handbooks; and

vii. Ensure outsourced services employ adequate ISCM to protect the confidentiality, integrity, and availability of DOC information and information systems.

4.1.18 System and Communications Protection

Bureaus must protect information within systems and during transit in accordance with the security categorization and sensitivity of the information. Bureaus must:

i. Ensure separation of general users' activities from those of privileged users and/or system functions. The separation of these functions can be implemented by physical or logical security controls;

ii. Secure all physical or logical connections between information systems, networks, or Bureau's information systems and networks by or through a DOC Trusted Internet Connection (TIC);[14]

iii. Provide services only through a secure connection and implement privacy and integrity protections available for publicly accessible DOC websites, web services, and web connections;

iv. Block or restrict access to known malicious resources and sites using boundary protection devices;

v. Monitor, control, and protect communications (e.g., information transmitted or received by DOC information systems) at the external boundaries and key internal boundaries of the information systems; and

vi. Use approved cryptographic mechanisms to protect the confidentiality and integrity of Data at Rest (DAR), Data in Transit (DIT), and Data in Use (DIU).

4.1.19 System and Information Integrity

Bureau information systems must be able to identify, report, and correct system flaws to support the DOC enterprise-wide cybersecurity and risk management program. Bureaus must:

[13] PM 2015-08, *Supply Chain Risk Assessment (SCRA) Requirements for the Acquisition of Moderate Impact and High Impact Information Systems.*

[14] Bureaus implementing TIC 3.0 must ensure effective monitoring controls are in place to support the Department's TIC Working Group guidance.

i. Test and install software and firmware updates related to flaw remediation for effectiveness and potential side effects;

ii. Identify, monitor, and report accurate information and information system flaws;

iii. Implement malicious code and anti-virus protections within the information systems;

iv. Monitor information system security alerts, advisories, and take appropriate response actions;

v. Limit information system error messages to explicitly provide information necessary for corrective actions without revealing information that could be exploited; and

vi. Install security-relevant software and firmware updates.

4.1.20 Supply Chain Risk Management

The DOC Supply Chain Risk Management (SCRM) Program oversees supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of system components or system services within the Department. Bureaus must:

i. Establish processes to identify and address weaknesses or deficiencies in information systems impacted by supply chain concerns;

ii. Employ supply chain security controls to protect against supply chain risks to the information system, data, and/or service to limit the harm or consequences from supply chain related events;

iii. Document implementation of supply chain security controls in the SSPP for the information system; and

iv. Assess and update the supply chain-related risks associated with suppliers or contractors, and/or system services.

4.2 Use of DOC IT Resources Outside the United States

Requests to transport DOC desktop computers, laptop computers, mobile devices, and servers outside the U.S. must be documented and approved, in writing, by the Bureau CISO or their designee and these approvals must be made available for review by the DOC CISO, upon request. Bureaus must:

i. Ensure any additional approvals necessary to transport DOC assets outside of the U.S. are received prior to travel;

ii. Limit information taken outside the U.S. to that which is needed to accomplish the purpose of the travel;

iii. Prevent access to DOC information systems and email from outside the U.S., with the exception of approved systems, hardware, and assets; and

iv. Inspect computers, smartphones, and any other device or media that have been transported outside the U.S. for compromise prior to any physical or logical connection to any DOC information system.

Appendix A: AUTHORITIES AND FEDERAL MANDATES

A.1 Laws

- Circular No. A-130 Managing Information as a Strategic Resource 2016
- Clinger-Cohen Act of 1996 (40 U.S.C. 11101(6))
- Computer Fraud and Abuse Act of 1986 (18 U.S.C. 1030 et seq.)
- Cybersecurity Information Security Sharing Act of 2015 (P.L. 114-113, Div. N)
- E-Government Act of 2002 (P.L. 107-347)
- Electronic Communications Privacy Act of 1986 (18 U.S.C. 2510 et seq., 2701 et seq., 3121 et seq.)
- Federal Information Security Modernization Act (FISMA) of 2014 (44 U.S.C. 3541 - 3549)
- Federal Information Technology Acquisition Reform Act (FITARA) (P.L. 113-291, Title VIII, Subtitle D)
- National Cybersecurity Protection Act of 2014 (P.L. 113-282)
- Paperwork Reduction Act (PRA) of 1995, as amended (44 U.S.C. 3501-3519)
- Privacy Act of 1974, as amended (5 U.S.C. 552a, as amended)
- Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act or the ”SECURE Technology Act” (P.L. 115-390)

A.2 Federal Mandates

- Binding Operational Directive (BOD) 16-03: 2016 Agency Cybersecurity Reporting Requirements
- BOD 16-02: Threat to Network Infrastructure Devices
- BOD 17-01: Removal of Kaspersky-branded Products
- BOD 18-01: Enhance Email and Web Security
- BOD 18-02: Securing High Value Assets
- BOD 19-02: Vulnerability Remediation Requirements for Internet-Accessible Systems
- BOD 20-01: Develop and Publish a Vulnerability Disclosure Policy
- BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities
- FIPS 140-2: Security Requirements for Cryptographic Modules
- FIPS 199: Standards for Security Categorization of Federal Information and Information Systems
- FIPS 200: Minimum Security Requirements for Federal Information and Information Systems

- FIPS 201-3: Personal Identity Verification (PIV) of Federal Employees and Contractors
- National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/ HSPD-23), Cybersecurity Policy
- OMB Circular No. A-11: Preparation, Submission, and Execution of the Budget
- OMB Circular No. A-130: Management of Federal Information Resources
- OMB M-02-01: Guidance for Preparing and Submitting Security Plans of Action and Milestones
- OMB M-03-22: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
- OMB M-15-13: Policy to Require Secure Connections Across Federal Websites and Web Services
- OMB M-15-14: Management and Oversight of Federal Information Technology
- OMB M-19-03: Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program
- OMB M-19-17: Enabling Mission Delivery through Improved Identity, Credential, and Access Management
- OMB M-19-26: Update to the Trusted Internet Connections (TIC) Initiative
- OMB M-21-30: Protecting Critical Software Through Enhanced Security Measures
- OMB M-21-31: Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incident
- OMB M-22-01: Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response
- OMB M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

A.3 Department Mandates

- Department Administrative Order (DAO) 200-0: Department of Commerce Handbooks and Manuals
- Department Administrative Order (DAO) 207-1: Security Programs
- Department Organizational Order (DOO) 15-23: Chief Information Officer
- DOO 20-31: Chief Privacy Officer and Director of Open Government

Appendix B: ACRONYMS

Acronym	Definition
ATO	Authority to Operate
BIA	Business Impact Analysis
BOD	Binding Operational Directive
CCP	Common Controls Program
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNSS	Committee on National Security Systems
COOP	Continuity of Operations Plan
CPIC	Capital Planning and Investment Control
CSAM	Cyber Security Assessment and Management
CSF	Cyber Security Framework
CSP	Cloud Service Provider
DAO	Department Administrative Order
DAR	Data at Rest
DHS	Department of Homeland Security
DIT	Data in Transit
DIU	Data in Use
DOC	Department of Commerce
DOO	Department Organizational Orders
DRP	Disaster Recovery Plan
ECP	Enterprise Cybersecurity Policy
ESOC	Enterprise Security Operations Center
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act of 2014
FITARA	Federal Information Technology Acquisition Reform Act

Acronym	Definition
GAO	Government Accountability Office
HSPD	Homeland Security Presidential Directive
IC	Intelligence Community
ICD	Intelligence Community Directives
IRP	Incident Response Plan
ISA	Interconnection Security Agreement
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Plan
IT	Information Technology
ITSBP	Information Technology Security Baseline Policy
MFA	Multifactor Authentication
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSI	National Security Information
NSS	National Security Systems
OCRM	Office of Cybersecurity and IT Risk Management
OIG	Office of Inspector General
OMB	Office of Management and Budget
ONCD	Office of the National Cyber Director
OPM	Office of Personnel Management
OPOG	Office of Privacy and Open Government
OSY	Office of Security
PBX	Private Branch Exchange
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification

Acronym	Definition
POA&M	Plan of Action and Milestones
PTA	Privacy Threshold Analysis
RD	Restricted Data
RMF	Risk Management Framework
SAISO	Senior Agency Information Security Officer
SAOP	Senior Agency Official for Privacy
SAR	Security Assessment Report
SCI	Sensitive Compartmented Information
SCRM	Supply Chain Risk Management
SDLC	System Development Lifecycle
SORN	System of Record Notice
SP	Special Publication
SPAA	Security and Privacy Assessment and Authorization
SPCM	Security and Privacy Control Matrix
SSPP	System Security and Privacy Plan
TIC	Trusted Internet Connection
U.S.	United States
ZTA	Zero Trust Architecture

Appendix C: GLOSSARY

Term	Definition
Agency	In the context of this document, the term "agency" almost always refers to the Department of Commerce, unless otherwise specified.
Assessment	Usually refers to a Security Assessment (see below), unless otherwise specified.
Audit	The independent examination of records and activities to ensure compliance; establish controls, policy, and operational procedures, and to recommend indicated changes in controls, policy, or procedures.
Authority to Operate	The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls.
Authorization	The granting of access rights to a user, program, or process. See also Authorization (to operate) and Authorization and Accreditation for authorization specific to information systems.
Availability	The property of an information system or service that ensures timely and reliable access to and use of that information system or service and the information it contains.
Bureau	As defined by DOO 1-1, the operating units of the Department are organizational entities outside the Office of the Secretary charged with carrying out specified substantive functions (i.e., programs) of the Department.
Classified Information	Information that has been determined: (i) pursuant to Executive Order 12958 as amended by Executive Order 13526, or any predecessor Order, to be classified national security information; or (ii) pursuant to the Atomic Energy Act of 1954, as amended, to be Restricted Data (RD).
Cloud Service(s)	Refers to a wide range of services delivered on demand to companies and customers over the internet. These services are designed to provide easy, affordable access to applications and resources, without the need for internal infrastructure or hardware.
Confidentiality	The property of an information system or service that preserves authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Connection	The action of two or more devices successfully sending and receiving information. It can also mean the link between a plug or connector into a port or jack.
Control Parameter	The variable part of a control or control enhancement that is instantiated by an organization during the tailoring process by either assigning an organization-defined value or selecting a value from a predefined list provided as part of the control or control enhancement.

Term	Definition
Countermeasures	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
DOC-Approved Tools	A software product and/or technology that is either a) Specified in an Approved standard, b) Adopted in an Approved standard and specified either in an appendix of the Approved standard or in a document referenced by the Approved standard, or c) Specified in the list of Approved security functions.
Impact	The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the U.S.) of a loss of confidentiality, integrity, or availability of information or an information system.
Information	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including, but not limited to textual, numerical, graphic, cartographic, narrative, or audiovisual.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Integrity	The property of an information system or service that guards against unauthorized modification or destruction of information (intentional or otherwise). Includes ensuring information non-repudiation and authenticity.
Mobile Device	A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and e-readers.

Term	Definition
Network	Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
Non-local Maintenance	Maintenance activities conducted by individuals communicating through an external network (e.g., the Internet). Any act that either prevents the failure or malfunction of equipment or restores its operating capability performed via the network, without being physically present.
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.
Privacy Impact Assessment	[OMB Memorandum 03-22] An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
Risk	A measure of the extent to which an organization is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security and privacy controls planned or in place. Synonymous with risk analysis.
Security Assessment	The testing or evaluation of security and privacy controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.
Security and Privacy Assessment and Authorization	The process of conducting a security assessment on an information system (see Security Assessment above) and determining, based on the results of that assessment, whether the information system should be given authorization to operate.

Term	Definition
Security Assessment Report	DOC-mandated documentation of findings in a risk assessment.
Security Categorization	The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS Publication 199 for other than national security systems. See Security Category.
Security Control	A safeguard or countermeasure prescribed for an information system, or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.
Security Requirement	A requirement levied on an information system or an organization that is derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, and/or mission/business needs to ensure the confidentiality, integrity, and availability of information that is being processed, stored, or transmitted.
System Owner	Mid-level manager responsible for day-to-day information system operations and responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
System Security and Privacy Plan	Formal document that provides an overview of the security requirements for an information system and describes the security and privacy controls in place or planned for meeting those requirements.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, modification of information, and/or Denial of Service.
Trusted Internet Connections	TIC is a Federal cybersecurity initiative intended to consolidating network connections and enhancing visibility and security measures throughout the Federal network.
User	Federal employees or contractors, guest researchers, collaborators, or others requiring access to and use of DOC information, information systems or information resource, including accessing an information system either by direct connections (e.g., via terminals) or indirect connections (e.g., prepare input data or receive output that is not reviewed for content or classification by a responsible individual) and access via a process.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Web Service	A software component or system designed to support interoperable machine- or application- oriented interaction over a network. A Web service has an interface described in a machine-processable format. Other systems interact with the Web service in a manner prescribed by its description using SOAP messages, typically

Term	Definition
	conveyed using HTTP with an XML serialization in conjunction with other Web-related standards.