




Approved On:

DOJ Order

CYBERSECURITY PROGRAM

- PURPOSE:** Maintains and enhances the Department of Justice (Department or DOJ) Cybersecurity Program as established in previous DOJ Orders; provides the governance framework for uniform policy; ensures appropriate privacy protections for DOJ information and information system security; confirms authorities; and assigns responsibilities for protecting information and information systems that store, process, or transmit DOJ electronic information from cyber intrusions.
- SCOPE:** All DOJ components, personnel, and information systems that process, store, or transmit DOJ national security or unclassified information; contractors and other users and operators of information systems that support the operations and assets of DOJ, including any non-DOJ organizations and their representatives who are granted access to DOJ information resources, such as other federal agencies and cloud providers.
- ORIGINATOR:** Justice Management Division (JMD), Office of the Chief Information Officer
- CATEGORY:** (I) Administrative, (II) Information Technology; Information and Privacy
- AUTHORITY:** Federal Information Security Modernization Act of 2014, Pub. L. 107-347, 116 Stat. 2899 (Dec. 18, 2014) (primarily codified at 44 United States Code (U.S.C.) chapter 35, subchapter II); Office of Management and Budget Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016, reference Appendix A for additional authorities
- CANCELLATION:** DOJ Order 2640.2F
- DISTRIBUTION:** Electronically distributed to those referenced in the “SCOPE” section and posted on the DOJ directives electronic repository (SharePoint) at <https://doj365.sharepoint.us/sites/jmd-dm/dm/SitePages/Home.aspx>
- APPROVED BY:** *Lisa Monaco*
Deputy Attorney General 
-

ACTION LOG

The issuing component must review its DOJ directives at least every five years and make revisions as necessary. The action log records dates of approval, recertification, and cancellation, as well as major and minor modifications to this directive, and provides a brief summary of all revisions. In the event this directive is cancelled, superseded, or supersedes another directive, that will also be noted in the action log.

Action	Authorized by	Date	Summary
Reissuance	Lee J. Lofthus Assistant Attorney General for Administration	9/15/2016	Reflected updated security requirements for DOJ information and information systems.
Update	Lisa Monaco Deputy Attorney General <i>Lisa Monaco</i>	<i>11/17/2023</i>	Updated to align with new federal mandates, directives, and guidance.

TABLE OF CONTENTS

ACTION LOG.....	2
DEFINITIONS.....	4
ACRONYMS.....	10
I. Policy.....	13
A. Maintains Staff to Serve as the Central Focal Point for Cybersecurity.....	13
B. Deploys and Manages a Department-Wide Common Security Strategy.....	14
C. Identifies New and Emerging Technologies.....	14
D. Develops Cybersecurity Policies, Standards, Procedures, and Templates.....	14
E. Promotes Awareness of Security and Privacy Risks and Policies.....	14
F. Develops Standards for and Performs Security and Privacy Control Monitoring and Evaluation.....	15
G. Develops and Manages a Comprehensive Risk Management Program.....	15
H. Maintain System Inventory and Security and Privacy Authorization Documentation.....	16
I. Manage Supply Chain Risk Management Program.....	16
J. Maintain Enterprise High Value Asset Governance.....	16
K. Protects the Privacy of Individuals.....	17
II. Information System Security and Privacy Requirements.....	17
A. Security and Privacy Control Families.....	18
B. Contractor Access to Information Systems.....	32
C. Use of DOJ IT Resources Outside the United States.....	33
D. Classified Information.....	33
E. Cloud Computing.....	34
F. Protection of Mobile Devices and Removable Media.....	35
G. External Information Systems.....	35
H. Wireless Communication Platforms.....	35
III. Roles and Responsibilities.....	36
A. DOJ Chief Information Officer.....	36
B. DOJ Chief Information Security Officer.....	37
C. Department Security Officer.....	39
D. Head of Component or Designee(s).....	39
E. Chief Privacy and Civil Liberties Officer.....	41
APPENDIX A: AUTHORITIES.....	44

DEFINITIONS

Term	Definition
Access, Internal	Either local access or internal network access to DOJ information systems. Local access is access to information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (e.g., non-local accesses). Internal networks include local area networks and wide area networks.
Access, Public	Limited to non-DOJ users of DOJ information systems. In accordance with the E-Authentication E-Government initiative, authentication of non-DOJ users accessing federal information systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Components must use risk assessments to determine authentication needs and consider scalability, practicality, and security in balancing the need to ensure ease of use for access to federal information and information systems with the need to protect and adequately mitigate risk. Components may allow a limited number of user actions without identification or authentication, including access to public websites or other publicly accessible federal information systems.
Access, Remote	Any access to a DOJ non-public information system by a DOJ employee or contractor operating outside the authorization boundary of the organizational system and communicating through an external, non-DOJ-controlled network. Remote access presents additional security concerns as the component has no direct control over the application of required security and privacy controls or the assessment of security control effectiveness of the connecting devices and network. The goal of these requirements is to ensure that components can safely use remote access to better accomplish their missions.
Access, General	Authorized general information system access that is approved access and that is not privileged access.
Access, Privileged	Authorized privileged information system access that is approved access with elevated roles or functions – especially security-relevant functions (e.g., account management, system administration, and application configuration) – and specifically restricts access to email and internet services.

Term	Definition
Authorization to Operate	The official management decision is given by an Authorizing Official or other designated senior DOJ official to authorize the operation of an information system and to explicitly accept the risk to DOJ operations, assets, individuals, other organizations, and the Nation.
Authorizing Official	A senior Federal official or executive with authority to assume formal responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
Breach	The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence in which (1) a person other than an authorized user accesses or potentially accesses Personally Identifiable Information (PII) or (2) an authorized user accesses or potentially accesses PII for an unauthorized purpose.
Cloud Computing	A model for enabling ubiquitous, 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 service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145, <i>The NIST Definition of Cloud Computing</i> .
Component	An office, board, division, or bureau of the Department of Justice as defined in 28 C.F.R. Part 0 Subpart A, Paragraph 0.1.
Continuous Monitoring	Maintaining ongoing awareness to support organizational risk decisions.
Critical Software	Any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes: is designed to run with elevated privilege or manage privileges; has direct or privileged access to networking or computing resources; is designed to control access to data or operational technology; performs a function critical to trust; or operates outside of normal trust boundaries with privileged access.
Cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Term	Definition
Data	Information in an electronic format that allows it to be retrieved or transmitted.
External Information System	An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security and privacy controls or the assessment of security control effectiveness.
Government-Authorized Device	Any device that exists within the authorization boundary of a DOJ information system with an Authorization to Operate. This includes, but is not limited to, equipment furnished by the government.
Head of Component	The Director or Administrator of a bureau or the Assistant Attorney General or equivalent of the offices, boards, and divisions.
Incident	An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the availability, integrity, authentication, confidentiality, or nonrepudiation ¹ of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
Information	Any communication or representation of knowledge, such as facts, data, or opinions, in any form or medium, including textual, numerical, graphic, cartographic, narrative, or audio-visual. This includes communication or representation of knowledge in an electronic format that allows it to be stored, retrieved, or transmitted.
Information, DOJ	Information that is owned, produced, controlled, protected by, or otherwise within the custody or responsibility of DOJ, including information related to DOJ programs or personnel. It includes information (1) provided by, generated by, or generated for DOJ, (2) provided to DOJ and in DOJ custody, or (3) managed or acquired by a DOJ contractor in connection with the performance of a contract regardless of format.
Information System	A discrete set of information resources organized for collecting, processing, maintaining, using, sharing, disseminating, or disposing of information. Information systems include specialized systems such as industrial/process control systems, telephone switching and private branch exchange systems, and environmental control systems.

¹ Protection against an individual who falsely denies having performed a certain action and provides the capability to determine whether an individual took a certain action, such as creating information, sending a message, approving information, or receiving a message. NIST SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, Appendix A.

Term	Definition
Information System Security Officer	An individual with assigned responsibility for maintaining the appropriate operational security level for an information system or program.
Insider	Any person with authorized access to any U.S. Government resource including personnel, facilities, information, equipment, networks, or systems.
Insider Threat	The threat that an insider will use their authorized access, wittingly or unwittingly, to do harm to the security of the U.S. This threat can include damage to the U.S. through espionage, terrorism, unauthorized disclosure of information, or the loss or degradation of departmental resources or capabilities.
Least Functionality	The security concept in which information systems are configured to provide only essential capabilities and specifically prohibit or restrict the use of non-essential functions, such as ports, protocols, and/or services that are not integral to the operation of that information system.
Least Privilege	The security concept in which a user or process is given the minimum levels of access or permissions needed to perform their job or intended function.
Multifactor Authentication	Authentication using two or more factors to achieve authentication. Factors include: (i) something the user knows (e.g., password/personal identification number [PIN]); (ii) something the user has (e.g., cryptographic identification device, token); or (iii) something the user is (e.g., biometric). ²
National Security Information	Information that has been determined (pursuant to Executive Order 13526, <i>Classified National Security Information</i> , December 29, 2009, or any successor order, or by the <i>Atomic Energy Act of 1954</i>) to require protection against unauthorized disclosure and is marked to indicate its classified status.

² The Department's default multifactor authentication is using Personal Identity Verification (PIV) as the second form factor.

Term	Definition
Policy Enforcement Point	As described and used within NIST SP 800-207, <i>Zero Trust Architecture</i> ; a system responsible for enabling, monitoring, and eventually terminating connections between end users, applications or other non- human entities, and enterprise resources.
Personally Identifiable Information (PII)	<p>Information that can be used to distinguish or trace an individual’s identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth or mother’s maiden name.</p> <p>To determine whether the information is PII, the agency must perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. When performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available – in any medium and from any source – that would make it possible to identify an individual.³</p>
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically it is a function of (1) the adverse impact or magnitude of the harm that would arise if the circumstance or event occurs; and (2) the likelihood of occurrence. Risk can include both information security and privacy risks.
Risk Management	The process of managing risks to DOJ operations (including mission, functions, image, or reputation), DOJ assets, data, individuals, and other organizations that result from the operation of an information system. The process includes: (1) the conduct of a risk assessment; (2) the implementation of a risk mitigation strategy; and (3) the employment of techniques and procedures for the continuous monitoring of the security state of the information system.

³ OMB Circular A-130, *Managing Information as a Strategic Resource*, (July 28, 2016), II-1 to II-2.

Term	Definition
Security and Privacy Continuous Monitoring Strategy	A formal document that catalogs the available security and privacy controls implemented at DOJ across the DOJ risk management tiers. It supports the effective monitoring of controls on an ongoing basis by assigning a DOJ-defined assessment frequency to each control that is sufficient to ensure compliance with applicable security and privacy requirements and to maintain an ongoing awareness of information security and privacy vulnerabilities and threats to support organizational risk management decisions.
Senior Component Official for Privacy	The Senior Component Official for Privacy (SCOP) role and responsibilities are defined in DOJ Order 0601, <i>Privacy and Civil Liberties</i> , or a successor order. Generally, a component’s SCOP holds primary responsibility for the applicable component’s privacy and civil liberties activities, including compliance with applicable privacy laws, regulations, directives, and policies.
System Security and Privacy Plan	A formal document that details (1) the security and privacy controls selected for an information system or environment of operation that are in place, or planned, for meeting applicable security and privacy requirements and managing security and privacy risks; (2) how the controls have been implemented; and (3) the methodologies and metrics that will be used to assess the controls.
Terminal Services	A multi-user, thin client environment. The user’s machine functions like an input/output terminal to the central server.
United States	Includes the land area, internal waters, territorial sea, and airspace of the United States, including: (1) United States territories; and (2) other areas over which the U.S. Government has complete jurisdiction and control or has exclusive authority or defense responsibility.
Virtual Private Network	Enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. A virtual private network is created by establishing a virtual point-to-point connection using dedicated connections, virtual tunneling protocols, and traffic encryption.

ACRONYMS

Acronym	Meaning
AAG/A	Assistant Attorney General for Administration
AG	Attorney General
AO	Authorizing Official
APN	Acquisition Policy Notice
ATO	Authorization to Operate
BIA	Business Impact Analysis
CD	Compact Disc
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CMT	Core Management Team
CNSS	Committee on National Security Systems
COR	Contracting Officer's Representative
CPCLO	Chief Privacy and Civil Liberties Officer
CSAT	Cybersecurity Awareness and Training
CSP	Cloud Service Provider
CSS	Cybersecurity Services Staff
DAAG/IRM	Deputy Assistant Attorney General/Information Resources Management
DAG	Deputy Attorney General
DAR	Data at Rest
DIT	Data in Transit
DNI	Director of National Intelligence
DNS	Domain Name System
DOJ	Department of Justice
DSO	Department Security Officer
DVD	Digital Video Disc

Acronym	Meaning
EDR	Endpoint Detection and Response
ERM	Enterprise Risk Management
FBI	Federal Bureau of Investigation
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FITARA	Federal Information Technology Acquisition Reform Act
GAO	Government Accountability Office
HTTPS	Hypertext Transfer Protocol Secure
HVA	High Value Asset
ICAM	Identity, Credential, and Access Management
ICD	Intelligence Community Directive
ICTS	Information and Communication Technology Services
IG	Inspector General
IPA	Initial Privacy Assessment
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Plan
IT	Information Technology
ITPDP	Insider Threat Prevention and Detection Program
JAR	Justice Acquisition Regulations
JCAM	Joint Cybersecurity Authorization Management
JCOTS	Justice Cloud Optimized TIC Service
JEFS	Justice Enterprise File Sharing
JSOC	Justice Security Operations Center
MFA	Multifactor Authentication
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSI	National Security Information
NSS	National Security Systems
OCIO	Office of the Chief Information Officer

Acronym	Meaning
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OPCL	Office of Privacy and Civil Liberties
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
PTA	Privacy Threshold Analysis
RMF	Risk Management Framework
SCI	Sensitive Compartmented Information
SCOP	Senior Component Official for Privacy
SCRM	Supply Chain Risk Management
SDLC	Systems Development Lifecycle
SORN	System or Records Notice
SP	Special Publication
SPAA	Security and Privacy Assessment and Authorization Handbook
SPDR	Security Posture Dashboard Report
SPE	Senior Procurement Executive
SPOM	Security Program Operating Manual
SSN	Social Security Number
TIC	Trusted Internet Connection
UAS	Unmanned Aircraft System
USB	Universal Serial Bus
VPN	Virtual Private Network
U.S.C.	United States Code

I. Policy

The *Federal Information Security Modernization Act of 2014* (FISMA) and the Office of Management and Budget (OMB) *Circular A-130* require the Department of Justice to maintain a DOJ-wide Cybersecurity Program that protects DOJ information systems and operations; maximizes resources; and establishes the governance framework, policy requirements, and standards for managing the security and privacy of departmental electronic information, information systems, and associated assets.

In accordance with these requirements, this Order establishes and explicates the DOJ Cybersecurity Program (formerly established by DOJ Order 2640.2F, *Information Technology Security*). Through this Cybersecurity Program, DOJ must continue to safeguard the Department against malicious unauthorized access, use, disclosure, disruption, modification, or damage or destruction of its information systems and resources in support of DOJ's mission. FISMA directs agency heads to delegate authority to the agency Chief Information Officer (CIO), who is required to designate a senior agency information security officer to carry out the CIO's responsibilities under FISMA.⁴ The DOJ CIO has designated the DOJ Chief Information Security Officer (CISO) under this authority, and the CIO maintains the authority to further designate cybersecurity responsibilities as necessary within the Office of the CIO (OCIO) or to other qualified and appropriate DOJ officials.

The Chief Privacy and Civil Liberties Officer (CPCLO), supported by the Office of Privacy and Civil Liberties (OPCL), serves as the central focal point for privacy in DOJ. The DOJ CIO, CISO, and cybersecurity personnel must coordinate with the CPCLO, OPCL, and the relevant Senior Component Official for Privacy (SCOP) on privacy risks.

The DOJ CISO manages and oversees the Cybersecurity Program. In that capacity, the CISO is responsible for ensuring that DOJ complies with the following Cybersecurity Program requirements:

A. Maintains Staff to Serve as the Central Focal Point for Cybersecurity

The Cybersecurity Services Staff (CSS) serves as DOJ's central focal point for cybersecurity. CSS provides DOJ-wide management and implementation of the DOJ Cybersecurity Program. CSS and the components work collaboratively to manage the priorities for achieving business objectives and complying with the required laws, rules, and regulations, including those listed in Appendix A; Directives; Presidential Decision Directives/Presidential Directives; Presidential Executive Orders; OMB circulars and memoranda; National Institute of Standards and Technology (NIST) requirements; Committee on National Security Systems (CNSS) requirements;

⁴ 44 U.S.C. § 3554(a)(3).

Director of National Intelligence (DNI) directives; and DOJ cybersecurity requirements.

B. Deploys and Manages a Department-Wide Common Security Strategy

The DOJ CIO sets and implements the Department's common security strategy that defines security goals for the components in alignment with applicable federal laws, regulations, and guidance. These goals outline DOJ's security posture, both internally and externally, while considering each component's respective business needs and missions. DOJ's common security strategy is strengthened by adopting an enterprise security architecture to ensure that information technology (IT) and supporting infrastructure remain secure throughout the entire lifecycle. Components must align information system security requirements to the strategy and security architecture at the beginning of the system's development lifecycle (SDLC) and appropriately fund such security requirements.

C. Identifies New and Emerging Technologies

The increase in the volume of departmental electronic information is so substantial and dynamic that DOJ is constantly identifying new and emerging technologies to assist in accomplishing its evolving national and global mission. Components must coordinate with CSS before implementing new or emerging technologies that will or may impact the DOJ enterprise architecture.⁵ To deviate from the DOJ enterprise architecture or have overlapping enterprise security services provided by OCIO, components must obtain a waiver from the DOJ CIO.

D. Develops Cybersecurity Policies, Standards, Procedures, and Templates

DOJ's cybersecurity policies, standards, procedures, and templates address DOJ's information system security and privacy needs and serve as the foundation for DOJ's Cybersecurity Program. The cybersecurity policies, standards, procedures, and templates are the primary mechanism for CSS senior management to communicate its cybersecurity requirements to the components. The DOJ CISO revises these cybersecurity policies, standards, procedures, and templates as necessary to align with federal mandates, directives, and guidance while allowing components to execute their missions.

E. Promotes Awareness of Security and Privacy Risks and Policies

The DOJ CISO must continually educate DOJ information system users on security and privacy risks and related policy. CSS will continually work with components to educate and provide resources to promote cybersecurity awareness training to users

⁵ See DOJ Policy Statement 0903.02, *Information Technology Enterprise Architecture Oversight*.

through its enterprise awareness and training materials and applications.

F. Develops Standards for and Performs Security and Privacy Control Monitoring and Evaluation

The DOJ CISO and CPCLLO must continually monitor and assess DOJ's cybersecurity and privacy programs to validate the security and privacy controls implemented to ensure effectiveness in safeguarding DOJ information systems and information and in conforming with applicable federal laws, regulations, and guidance. They must incorporate the monitoring of control effectiveness and compliance with policy within the Information Security Continuous Monitoring (ISCM) program, including using automated tools when possible.

G. Develops and Manages a Comprehensive Risk Management Program

The DOJ CISO and components must develop, implement, and manage information systems based on a thorough examination of the risks identified in security and privacy control assessments and the potential impact the information system has on DOJ operations. FISMA, OMB Circular A-130, NIST Special Publication (SP) 800-37, *Risk Management Framework for Information Systems and Organizations*, and other federal guidance concepts are incorporated in the DOJ risk management program. It presents a formal, structured approach for developing risk assessments for information systems and provides a uniform standard for evaluating security and privacy risks affecting the availability, integrity, authentication, confidentiality, or nonrepudiation of DOJ information or information systems.

DOJ information system owners and cybersecurity managers must adhere to the DOJ risk management program when assessing risks, framing risks, and prioritizing resources for the security and privacy assessment and authorization of information systems. Effective risk management must include risk identification and prioritization, categorization of recommended safeguards, feasibility of implementation, and other risk management processes as defined in the *DOJ Security and Privacy Assessment and Authorization (SPAA) Handbook*. The DOJ CISO must continually evaluate the DOJ risk management strategy to address the current threats to DOJ information systems and information.

DOJ components must use the iterative NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, Risk Management Framework (RMF) steps zero through six as defined in the *DOJ SPAA Handbook* to enforce the risk management process where security and privacy risks are assessed, responded to, and monitored in support of DOJ's ISCM activities. DOJ implements a three-tier ISCM approach to assess, analyze, prioritize, monitor, and report security and privacy risks at the information system, component, and DOJ levels. For contractor-managed information systems, such as hosting providers and Cloud Service

Providers (CSPs), components must ensure that all contracts include security and privacy clauses specifying the DOJ risk management and assessment and authorization requirements.

DOJ components must develop, monitor, and implement Plan of Actions and Milestones (POA&Ms) to correct information system deficiencies and reduce or eliminate vulnerabilities per the *DOJ POA&M Management Guide*. DOJ component information system owners must use a POA&M to track and resolve vulnerabilities within an information system, component, or DOJ.

DOJ components must incorporate security and privacy system risks into the larger scope of DOJ's Enterprise Risk Management (ERM).⁶ Effective ERM balances achieving security and privacy objectives with optimizing limited resources to manage risks, rather than addressing risks in silos.

H. Maintain System Inventory and Security and Privacy Authorization Documentation

The DOJ CISO must ensure that components identify and document each information system inventory in DOJ's Joint Cybersecurity Authorization Management (JCAM) application, the Department's enterprise record for security assessment and authorization. To effectively manage DOJ's FISMA inventory and automate reporting, components must associate information system assets to an information system authorization boundary. The components must certify the completeness and accuracy of their system inventory as stored in JCAM as part of the quarterly FISMA CIO metrics data call submission.

I. Manage Supply Chain Risk Management Program

The DOJ CISO must ensure that components conduct supply chain risk assessments consistent with federal mandates, directives, and guidance. The *DOJ Information and Communication Technology Services (ICTS) Supply Chain Risk Management (SCRM) Strategy*⁷ documents the organization, resources, responsibilities, processes, and artifacts that guide the secure procurement, deployment, and implementation of IT software, hardware, and services throughout the ICTS life cycle. The SCRM process must be a cooperative effort among procurement, cybersecurity, legal, IT operations, system stakeholders, and risk management officials.

J. Maintain Enterprise High Value Asset Governance

⁶ The DOJ Strategic Planning and Performance Staff manages the implementation of the ERM Program and leads the Department in the identification and management of enterprise risks that may have a significant impact on the performance and achievement of the Department's strategic objectives and strategies.

⁷ The Department has two ICTS SCRM programs; one operated by CSS within JMD that supports all non-FBI components, and a second operated solely by the FBI (because of its status as a member of the U.S. Intelligence Community).

The DOJ CISO must ensure that components identify and maintain an inventory of all designated High Value Assets (HVAs).⁸ DOJ components must complete security and privacy security control assessments for the information systems per the DOJ HVA Program to ensure the accuracy of information pertaining to the HVAs' security and privacy posture. DOJ components must develop and prioritize remediation of vulnerabilities associated with HVAs in accordance with the DOJ POA&M process.

K. Protects the Privacy of Individuals

While security and privacy are distinct disciplines, they are closely related. Therefore, the DOJ CISO and CPCLC must ensure that DOJ components take a coordinated approach to identifying and managing security and privacy risks while complying with security and privacy requirements.

In implementing the Cybersecurity Program, components and DOJ as a whole must ensure that they identify privacy needs and requirements at the beginning of the SDLC and fund them appropriately. Further, DOJ components must integrate the NIST RMF with DOJ's privacy program requirements under DOJ Order 0601, *Privacy and Civil Liberties*, May 14, 2020 (or its successor order), including the selection, implementation, assessment, and monitoring of privacy controls.

II. Information System Security and Privacy Requirements

The Justice Management Division's CSS has designed security and privacy controls to be technology neutral, focusing on the fundamental countermeasures needed to protect DOJ information and information systems. The security and privacy controls described in this Order apply to all DOJ information systems, information systems managed by contractors on behalf of DOJ, national security systems (NSS),⁹ and cloud services used by the Department.

DOJ information systems that process National Security Information (NSI) must meet additional requirements specified by the CNSS. DOJ information systems that process Sensitive Compartmented Information (SCI) must meet additional requirements established by the Office of the Director of National Intelligence (ODNI). If there is a

⁸ The HVA designation is not applicable to national security systems (NSS) as defined in FISMA (44 U.S.C. § 3552). Owners and operators of NSS, which includes those systems critical to the execution of military, intelligence, and cryptologic operations, shall follow all CNSS issuances, as well as Department of Defense (DoD) or IC guidance regarding the protection of sensitive information and systems with respect to NSS. If a situation arises whereby designating a system satisfies the conditions of both an NSS and HVA, the system shall be designated an NSS.

⁹ NSS shall include those systems defined as NSS in 44 U.S.C. § 3552(b)(6) as well as all other Department of Defense and Intelligence Community systems, as described in 44 U.S.C. § 3553(e)(2) and 3553(e)(3), unless explicitly stated otherwise. Components must use NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*, as a guide to ensure proper identification and inventory management of NSS.

conflict in requirements defined in this Order for systems processing NSI or SCI, the CNSS or DNI requirements govern.

The DOJ cybersecurity standards set forth below in subsections A through H require components to undertake specific actions at prescribed intervals to develop, implement, monitor, and manage the security and privacy controls implementation. Components that cannot meet these security and privacy controls must submit a waiver request from the component CIO or Head of Component designee to the DOJ CIO for approval. As several privacy controls are legal requirements and cannot be waived, the relevant SCOP must coordinate with OPCL or the CPCL to resolve any issues with privacy controls.

A. Security and Privacy Control Families

1. Access Control

Components must:

- i. Document and approve all logical access to information systems and system resources based upon need-to-know and the concept of least privileged;
- ii. Document, implement, and monitor security and privacy security measures to control the flow of information within the system and between interconnected systems;
- iii. Enforce and manage the separation of duties based on role and responsibilities; and
- iv. Display DOJ-approved warning banner to users before granting access to information systems.

DOJ allows three types of information system access: internal, remote, and public. Each type of access poses security challenges and has requirements and solutions, as noted below.

i. Internal access

Internal access is either local access or internal network access to non-public DOJ information systems. Components must:

- Limit internal access to non-public DOJ information systems to authorized users, processes acting on behalf of authorized users, or approved devices (including other information systems); and limit internal access to the types of transactions and functions permitted by authorized users;

- Prohibit automatic forwarding of DOJ information (*e.g.*, emails) received in a DOJ information system to or through a non-DOJ information system;
- Limit the physical locations in which non-public DOJ information systems, including cloud instances, may operate to those locations within the boundaries of the United States (which includes all states, federal districts, territories, and embassies); and
- Prohibit a non-U.S. citizen's general and privileged user access to IT resources unless the component CIO's waiver request has been approved by the DOJ CIO and the Department Security Officer (DSO).

ii. Remote access

Remote access is any access to non-public DOJ information systems by a DOJ employee or contractor communicating through a non-DOJ-controlled network. Components must:

- Follow the DOJ Identity, Credential, and Access Management (ICAM) requirements for general and privileged user access;
- Limit remote access to non-public DOJ information systems to government-authorized devices using an encrypted DOJ virtual private network (VPN) or DOJ-approved Policy Enforcement Point; and
- Prevent split-tunneling and implement security measures to prevent users from connecting remote-access devices to any other network when those devices are connected to a DOJ information system.

iii. Public access

Public access is any access that allows a direct connection to the Internet. There are two categories of public access, both of which must be restricted to only communicate over encrypted connections. Components must:

- Implement Hypertext Transfer Protocol Secure (HTTPS) encryption only, with HTTP Strict Transport Security (HSTS), as applicable, for data in transit for publicly accessible DOJ information systems (*e.g.*, justice.gov) that do not require user identification and authentication; and
- Limit access to authenticated users with a valid need-to-know for

information systems that allow direct access from the Internet (*e.g.*, LearnDOJ) to non-public DOJ information.

2. Awareness and Training

Components must:

- i. Ensure all users complete Cybersecurity Awareness and Training (CSAT) and CPCLO privacy awareness training, both at entry on duty and annually;
- ii. Ensure all users complete role-based training to carry out their assigned information system security and privacy-related duties and responsibilities;
- iii. Ensure all users sign a Rules of Behavior upon completion of security and privacy training;
- iv. Ensure all users complete phishing training and exercises to detect and report phishing attempts; and
- v. Retain security and privacy awareness training records until superseded or for a period of at least three years from the date the record is created.

3. Audit and Accountability

Components must:

- i. Create, protect, and retain information system audit records per the *DOJ Cybersecurity Standard*¹⁰ to enable security monitoring, analyzing, investigating, and reporting of unlawful, unauthorized, or inappropriate information system activity;
- ii. Ensure that actions of authenticated information system general users and privileged users can be uniquely traced to those users to enable accountability for their actions;
- iii. Configure information systems to audit, as applicable, all relevant logs

¹⁰ The DOJ Cybersecurity Standard details the controls described in NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*; DOJ-specific security controls for unclassified information and information systems in the Unclassified Security Control Matrixes for Revisions 4, available at https://dojnet.doj.gov/jmd/ocio/ocio-document_library/cs/2-DOJ_Policy_Instruction/unclassified-control-matrix.xlsx and Revision 5, available at https://dojnet.doj.gov/jmd/ocio/ocio-document_library/cs/2-DOJ_Policy_Instruction/DOJ-Cybersecurity-Standard-NIST-800-53-Rev5_Final.xlsx; and the CNSS Instruction 1253 and DOJ-specific controls for classified information and information systems in the Classified Security Control Matrix, available at https://dojnet.doj.gov/jmd/ocio/ocio-document_library/cs/2-DOJ_Policy_Instruction/classified-control-matrix.xlsx.

(examples include but are not limited to VPN, firewall event, intrusion detection/prevention systems, network, Endpoint Detection and Response (EDR), and antivirus events)¹¹; and

- iv. Provide the top-level agency security operations center, the Justice Security Operations Center (JSOC), with near-real-time electronic audit logging data feeds, access, and visibility through a method acceptable to the JSOC.

4. Assessment, Authorization, and Monitoring

Components must:

- i. Complete and obtain an Authorization to Operate (ATO) for all information systems before operations;
- ii. Reauthorize information systems before ATO expiration;
- iii. Complete all security and privacy assessment and authorization documentation before information system operation as required by the DOJ SPAA Handbook, which includes privacy impact assessments (PIAs) and system of records notices (SORNs), as applicable;
- iv. Use JCAM to record information system authorization documentation and security and privacy control assessments to manage implementation and compliance effectively;
- v. Develop, implement, and monitor POA&Ms designed to correct deficiencies and reduce or eliminate vulnerabilities in DOJ information systems;
- vi. Document, authorize, and monitor all information system interconnections before operational use;
- vii. Perform continuous monitoring on all information systems and maintain awareness of the information system security and privacy posture in support of DOJ's risk management program;
- viii. Perform asset tagging on all information system to component system authorization boundaries in JCAM;
- ix. Provide automated cybersecurity posture information (*e.g.*, information from hardware asset management, software asset management, configuration settings management, software vulnerability management, enterprise mobility management, and cloud configuration management) to

¹¹ As directed in OMB Memorandum 21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*.

DOJ's Security Posture Dashboard Report (SPDR); and

- x. Manage the security posture of information systems using JCAM and SPDR.

5. Configuration Management

Components must:

- i. Establish and maintain baseline configurations and inventories of DOJ information systems (including hardware, software, firmware, and documentation) throughout the SDLC in accordance with the *DOJ Configuration Management Plan*;
- ii. Maintain an inventory of critical software;¹²
- iii. Implement least privilege, network segmentation, and secure configuration security measures on critical software;
- iv. Establish a centralized configuration change control process and security impact analysis to properly evaluate, test, approve, and document proposed changes before being put into production;
- v. Limit information system changes only to authorized personnel;
- vi. Prohibit users from installing software without authorization;
- vii. Implement least functionality and disable the use of non-secure ports, services, and protocols; and
- viii. Establish and enforce security settings consistent with the information system operational requirements and validate those controls through DOJ-approved tools.

6. Contingency Planning

Components must:

- i. Establish, maintain, and effectively implement an Information System Contingency Plan (ISCP) for emergency response, alternate processing and storage sites, backup operations, and post-disaster recovery for DOJ information systems to ensure the availability of critical IT resources and continuity of operations in emergency situations;

¹² See Executive Order 14028, *Improving the Nation's Cybersecurity*, May 12, 2021, § 4, Enhancing Software Supply Chain Security.

- ii. Conduct and document Business Impact Analyses for information systems; and
- iii. Complete testing and training of the ISCP in accordance with the DOJ cybersecurity standards and *DOJ Information System Contingency Planning Guide*.

7. Identification and Authentication

Components must:

- i. Identify, document, and maintain current inventory of information system users, processes acting on behalf of users, and devices;
- ii. Ensure authentication and verification of identities of those users, processes, and devices before granting them access to DOJ information systems, consistent with applicable federal laws, regulations, and guidance (this does not apply to unauthenticated access to public information systems);
- iii. Implement multifactor authentication credentials, also referred to as MFA, that are verifier impersonation-resistant for all information systems; and
- iv. Use a DOJ CIO-approved Identity Provider for authentication to enterprise information systems and resources.

8. Incident Response

Components must:

- i. Notify the JSOC¹³ within one hour of discovery of a suspected¹⁴ or confirmed incident or breach;
- ii. Ensure contracts stipulate requirements for contractors to notify the Contracting Officer, Contracting Officer's Representative (COR), and JSOC (or component-level Security Operations Center) within one hour of discovering any suspected or confirmed incidents or breaches consistent with this Order, guidance issued by the CPCLC, NIST standards and guidelines, and the Cybersecurity and Infrastructure Security Agency (CISA) notification guidelines;

¹³ JSOC is responsible for reporting incidents to appropriate external authorities such as CISA and the National Security Manager.

¹⁴ Components should ensure that contracts include a low definitional threshold for what constitutes a "suspected incident." At a minimum, that definition should refer to any reasonable suspicion that an incident has or will occur.

- iii. Ensure contracts contain uniform and consistent stipulations for contractors to cooperate with all aspects of DOJ's investigation, assessment, mitigation, and recovery activities;
- iv. Ensure contracts include the language required by Justice Acquisition Regulations (JAR), and DOJ acquisition directives unless waived, in whole or in part, by the DOJ Senior Procurement Executive (SPE) with concurrence from the DOJ CIO and CPCLO;
- v. Ensure that contracts otherwise allow for the Department's compliance with this Order and DOJ Policy Statement 0904.02, *Incident and Breach Response Playbook*;
- vi. Establish an operational incident response and handling capability for DOJ information systems that includes adequate preparation, detection, analysis, containment, eradication, and recovery in coordination with the JSOC;
- vii. Follow DOJ Policy Statement 0904.02, *Incident and Breach Response Playbook*, and the *DOJ Incident Response Plan* to track, document, and report incidents or breaches to appropriate DOJ officials and/or authorities;
- viii. Coordinate all incident response actions with the JSOC and provide timely updates;
- ix. Coordinate with the JSOC to the degree of specificity appropriate under the circumstances, and include JSOC on all incident response communications with entities external to DOJ;
- x. Provide information to the JSOC consistent with the *DOJ Incident Response Plan* to support incident or breach response preparation, detection, analysis, containment, eradication, and recovery. Access to such information access shall be consistent with DOJ Order 0908, *Use and Monitoring of DOJ Information Technology, Information Systems, and Access to an Authorized Users' Electronic Information*;
- xi. Assist with digital forensic and other investigations on electronic devices or associated media when requested by the JSOC;
- xii. Complete incident response plan testing and provide training to users with assigned incident response roles and responsibilities;
- xiii. Maintain a chain of custody to record the handling and transfer of media and devices to support forensic and other investigations;

- xiv. Implement the DOJ CIO-approved EDR solution on all endpoints to increase JSOC visibility necessary to respond to advanced forms of cybersecurity threats; and
- xv. Participate in and follow DOJ Core Management Team instructions as directed in DOJ Policy Statement 0904.02, *Incident and Breach Response Playbook*.

9. Maintenance

Components must:

- i. Perform periodic and timely maintenance on DOJ information systems;
- ii. Approve and monitor non-local information system maintenance and diagnostic activities; and
- iii. Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct on-site and remote information system maintenance.

10. Media Protection

Components must:

- i. Protect information system media in all forms;
- ii. Use the Justice Enterprise File Sharing (JEFS) solution for sharing with non-DOJ entities unless the DOJ CIO approves another file-sharing solution;¹⁵
- iii. Encrypt all (unclassified and classified) data using Federal Information Processing Standards (FIPS)-validated or National Security Agency-(NSA) approved encryption, as appropriate;¹⁶
- iv. Limit access to DOJ information systems and DOJ information to authorized users;
- v. Properly mark system media indicating classification, handling caveats, and applicable distribution limitations;

¹⁵ Component use of other file-sharing solutions to meet mission needs not fulfilled by JEFS must be approved by the DOJ CIO and must have an ATO granted by the Component's AO.

¹⁶ This requirement includes information transported on removable media, such as universal serial bus (USB) drives, compact discs (CDs), digital video discs (DVDs), and on portable/mobile devices (such as laptop computers or smartphones), and includes information stored by a non-agency service such as a cloud or managed service.

- vi. Sanitize or destroy information system media before disposal or release for reuse in accordance with *DOJ Security Program Operating Manual* (SPOM); and
- vii. Stipulate in contracts for IT equipment that any such equipment must be sanitized in accordance with the DOJ SPOM before being removed from a component's physically protected facility.

11. Physical and Environmental Protection

Components must:

- i. Limit physical access to information systems, equipment, and the respective operating environments to authorized individuals and monitor and log such accesses;
- ii. Retain physical access records for a period of one year for unclassified facilities and five years for classified facilities;
- iii. Protect the physical facility and support infrastructure for information systems;
- iv. Provide supporting utilities for information systems;
- v. Protect information systems against environmental hazards; and
- vi. Provide appropriate environmental controls in facilities containing DOJ information systems and information.

12. Planning

Components must:

- i. Develop, document, implement, and update System Security and Privacy Plans for DOJ information systems that describe the implemented and planned security and privacy controls for the information systems; and
- ii. Establish rules of behavior for individuals who access information systems.

13. Program Management

Components must:

- i. Implement a component cybersecurity program consistent with this Order and *DOJ's Information Security Continuous Monitoring Strategy*;

- ii. In coordination with the DOJ Insider Threat Prevention and Detection Program (ITPDP), implement DOJ Order 0901, *Insider Threat*, and report insider threat concerns to the DOJ ITPDP;
- iii. Ensure adequate resourcing (*i.e.*, people, process, and technology) to implement, monitor, and assess security and privacy controls;
- iv. Implement a risk management program that is consistent with the DOJ enterprise risk management strategy; and
- v. Use DOJ's Common Controls Program and DOJ Privacy Common Controls Program to the extent feasible to reduce duplicative security and privacy control assessments and authorization efforts.

14. Personnel Security

Components must:

- i. Ensure that individuals occupying positions of responsibility within the component (including third-party service providers) are trustworthy and meet security criteria established by DOJ for those positions;
- ii. Ensure that only U.S. citizens are authorized to access DOJ information systems or assist in the development, operation, management, or maintenance of DOJ information systems, including providing information system support, unless the component CIO requests a waiver, and the DOJ CIO and the DSO approve the waiver, specifically allowing access or assistance by the non-U.S. citizen;
- iii. Ensure the protection of DOJ information and information systems during and after personnel actions, such as termination and transfer; and
- iv. Employ formal sanctions as appropriate for personnel failing to comply with DOJ security policy and procedures in accordance with applicable laws and regulations.

15. Personally Identifiable Information Processing and Transparency

Components must:

- i. Only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have authority to do so, and identify this authority in the appropriate notice (such as Privacy Act system of records notice, 5 U.S.C. § 552a(e)(4), or Privacy Act notice and PIA, *id.* § 552a(e)(3));

- ii. Implement effective controls for governance, monitoring, and risk management and assessment to demonstrate that they are complying with applicable privacy protection requirements and minimizing overall privacy risk;
- iii. Limit the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII to that which is legally authorized, relevant, and reasonably deemed necessary for the proper performance of agency functions;
- iv. Minimize the collection, maintenance, and use of Social Security Numbers (SSNs) to only those circumstances when required by law or when necessary for a specific authorized purpose. When the collection, maintenance, or use of SSNs is required or necessary, implement appropriate technical and physical safeguards to ensure the security of records containing SSNs, such as redacting or masking the data;
- v. Implement data minimization and retention processes to ensure, to the extent reasonably practicable, that PII is accurate, relevant, timely, and complete; and reduce use of all PII to the minimum necessary for the proper performance of authorized agency functions;
- vi. Retain PII for only as long as necessary to fulfill authorized agency purposes and in accordance with a National Archives and Records Administration-approved records disposition schedule;
- vii. Provide individuals with access to Privacy Act records about them and the ability to have such Privacy Act records corrected or amended pursuant to the Privacy Act;
- viii. Ensure that technical, physical, and administrative safeguards are in place to protect PII collected or maintained by components against loss, unauthorized access, or disclosure and that planning and responses to privacy incidents and breaches comply with OMB policies and guidance;
- ix. Confirm that specific privacy requirements comply with and operate within DOJ's enterprise architecture to ensure that risk is addressed, and information systems achieve the necessary levels of trustworthiness, protection, and resilience;
- x. Ensure that the CPCLLO, or a duly authorized official, is made aware in a timely manner of information systems that cannot be appropriately protected or secured, and ensure that such systems are given a high priority for an upgrade, replacement, or retirement;

- xi. Require, as appropriate, other agencies and entities with which the component shares PII to maintain the PII in an information system consistent with the NIST FIPS 199 security impact level determined by DOJ;
- xii. Impose, where appropriate, conditions (including the selection and implementation of particular security and privacy controls) that govern the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII through written agreements, including contracts, data use agreements, information exchange agreements, and memoranda of understanding;
- xiii. Document and implement policies and procedures consistent with this Order for privacy oversight of contractors and other entities, including ensuring appropriate vetting and access control processes for contractors and others with access to information systems containing DOJ information;
- xiv. Complete and comply with the final determination from an Initial Privacy Assessment¹⁷ as early as possible during the design and development of or any significant modification to a project in which the component knows it will, or is unsure whether it will, create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII;
- xv. Complete a PIA as required by DOJ policy, generally before procuring, developing, or implementing an information system or project that collect, maintain, or disseminate information in identifiable form;
- xvi. Ensure that any new electronic collections of information in identifiable form for ten or more persons are consistent with the Paperwork Reduction Act; and
- xvii. Publish updates for the SORNs as required by the *Privacy Act of 1974*.

16. Risk Assessment

Components must:

- i. Complete the security categorization of the information system, including identifying all information types that the information system processes, stores, and transmits;
- ii. Periodically assess the risk to departmental operations (including mission,

¹⁷ FBI refers to Initial Privacy Assessments (IPAs) as Privacy Threshold Analysis (PTA).

function, image, or reputation) and assets, individuals, other organizations, and the Nation resulting from DOJ information systems operation and the associated processing, storing, or transmitting of DOJ information;

- iii. Monitor and scan information systems for vulnerabilities in accordance with the *DOJ Vulnerability Management Plan*;
- iv. Timely remediate vulnerabilities identified from automated scans, security and privacy control assessments, and audits;
- v. Perform annual penetration testing on information systems with a security categorization of FIPS High or categorized as an HVA;
- vi. Maintain an inventory of Internet-accessible information systems and report the inventory to CSS; and
- vii. Ensure all Internet-accessible information systems are in scope for the DOJ Vulnerability Disclosure Program and continuous assessment service.

17. Systems and Services Acquisition

Components must:

- i. Allocate sufficient resources to appropriately protect DOJ information systems according to information and system risk level and consistent with applicable NIST guidance;
- ii. Employ SDLC processes that incorporate information system security considerations;
- iii. Ensure that new acquisitions of information systems include available security configurations consistent with the *DOJ Configuration Management Plan*;
- iv. Employ software usage and installation restrictions to ensure that software installed on DOJ information systems complies with applicable copyright laws and licensing agreements; and
- v. Ensure that third-party providers are contractually required to comply with this Order and all applicable DOJ security policies and employ adequate security measures to protect the information, applications, and services outsourced from DOJ in accordance with the JAR and DOJ acquisition directives.

18. Systems and Communications Protection

Components must:

- i. Secure all physical or logical connections between information systems, networks, or components of information systems and networks either using Justice Cloud Optimized TIC Service (JCOTS) or an approved OCIO Trusted Internet Connection (TIC) solution;
- ii. Provide service only through a secure connection and use the strongest privacy and integrity protection available for information systems that allow access from the public Internet;
- iii. Block JSOC provided list of known malicious indicators and sites at boundary protection devices and services. The DOJ CISO must approve exceptions to allow access to specific resources and/or sites on this list, and components must report such exceptions to the JSOC. Components with information systems that require exemption from this requirement in its entirety must seek and obtain a waiver from the DOJ CIO;
- iv. Monitor, control, and protect component communications (*e.g.*, information transmitted or received by DOJ information systems) at the external boundaries and key internal boundaries of the information systems and DOJ applications;
- v. Implement Data at Rest (DAR) and Data in Transit (DIT) encryption for all information systems using approved FIPS encryption standards to protect the confidentiality and integrity of data; and
- vi. Restrict the use of technologies or services (*e.g.*, encapsulation, tunneling, encryption) inconsistent with DOJ security enterprise architecture requirements (*e.g.*, firewalls, intrusion detection systems, antivirus systems, content scanning, and filtering systems) unless the DOJ CIO grants a waiver based upon assessed risk, mitigating controls, and operational requirements.

19. System and Information Integrity

Components must:

- i. Identify, report, and correct information and information system flaws in accordance with the DOJ cybersecurity standards and *DOJ Vulnerability Management Plan*;
- ii. Provide protection from malicious code at appropriate locations within DOJ information systems; and
- iii. Monitor information system security alerts and advisories and take

appropriate actions.

20. Supply Chain Risk Management

Components must:

- i. Adhere to DOJ's SCRM strategy¹⁸ to facilitate the supply chain risk management policy implementation and associated supply chain risk management controls;
- ii. Include SCRM vendor risk assessments in procurement decisions in accordance with the JAR, and DOJ acquisition directives; and
- iii. Employ supply chain risk management controls and continuous monitoring to protect against supply chain risks to the information system, system component, or system service and to limit the harm or consequences from supply chain-related events.

B. Contractor Access to Information Systems

Components may use contractors to design, develop, operate, and maintain information systems on their behalf. Components may grant contractors access to DOJ information systems and information to perform work specified by contract. Contractors may have access from component or DOJ-owned computers or from U.S.- based contractor-owned computers. Contractors may process DOJ information on contractor-owned equipment within or outside DOJ space. In all these situations, the contractors and their subcontractors, including all personnel, information systems, and devices, must comply with this Order. Contracts must include the relevant provisions and clauses required by the JAR and DOJ acquisition directives unless waived, in whole or in part, by the DOJ CIO, CPCLO, and DOJ SPE.

When the contract requires or allows contractors to use contractor information systems (whether to access DOJ information systems and information or to process or store DOJ information), the contract must require that the contractors' information systems be assessed, authorized, and operated pursuant to a valid ATO. The Authorizing Official (AO) must issue the authorization in accordance with the ATO requirements in this document and the *SPAA Handbook* for unclassified and NSS. Contractors who use individual devices under the contract must provide an inventory of such devices to the COR and operate such devices pursuant to the requirements explicated in this Order, including all incident response requirements. Contractor systems used in this manner are subject to the same data calls as other DOJ systems.

Upon termination of contract work, the DOJ Contractor must remove all DOJ data

¹⁸ See footnote 6.

from contractor-owned IT equipment. The contract's project manager must perform the certification of data removal and deliver a letter confirming certification to the contracting officer within 15 business days of the termination of the contract unless otherwise extended by the Contracting Officer or COR.

C. Use of DOJ IT Resources Outside the United States

The DOJ CISO must approve, in writing, either individually or by category, the transportation or use of DOJ desktop computers, laptop computers, and servers outside the United States. DOJ employees' use of DOJ mobile devices (*e.g.*, tablet devices and smartphones) outside the United States must follow the requirements in the *DOJ Mobile Device and Mobile Application Security Plan* and *DOJ IT Asset Foreign Travel Security Plan*. Components must:

- i. Ensure any additional approvals necessary to transport DOJ assets outside of the United States are received before travel;
- ii. Limit data taken outside the United States to that which is needed to accomplish the purpose of the travel;
- iii. Prevent access to DOJ information systems from outside the United States, except for systems authorized explicitly for such access and email via smartphones or other mobile devices; and
- iv. Inspect computers, smartphones, and any other media that have been transported outside the United States for compromise before any physical or logical connection to any DOJ system. If the component cannot conduct such an inspection, it must reimaged the computer or sanitize the media.

D. Classified Information

1. National Security Systems and Sensitive Compartmented Information

ODNI establishes a security policy for information systems processing collateral (*i.e.*, SCI). The DNI CIO establishes a security policy for systems processing SCI. The Federal Bureau of Investigation (FBI) CIO or designee will serve as the AO for all DOJ SCI systems. The certification authority, oversight, and coordination with the FBI for non-FBI SCI systems reside solely with the CSS.

Components must conform to the DOJ SPOM, Intelligence Community Directives, Intelligence Community Policy Guidance, Intelligence Community Policy Memorandums, Presidential Policies and Orders, and CNSS policies to manage the security of their NSS.

2. Standalone Classified Laptop, Mobile Computing Devices, and Removable Media

The Head of Component or principal deputy must provide in writing to the DOJ CIO through the DOJ CISO a request and justification to process classified information on standalone laptops, mobile computing devices, and removable media. Such approvals may be granted only upon implementing adequate technical protective measures as documented in the system authorization package and approved by the system AO.

3. Facsimile Transmission

All classified and sensitive facsimile transmissions must be preceded by a cover sheet that contains the classification or sensitivity of the information; the name, office, and voice/fax telephone numbers for the recipient(s) and sender; and a warning banner with instructions to the recipient if the facsimile was received in error.

4. Encryption

Classified information must be encrypted for transmission with NSA-approved encryption.

E. Cloud Computing

DOJ uses the definition documented in NIST SP 800-145, *The NIST Definition of Cloud Computing*, to designate cloud systems.¹⁹ Cloud-based information systems in use within DOJ must have an ATO and must adhere to the requirements identified in FISMA, NIST, and Federal Risk and Authorization Management Program (FedRAMP) documentation. Components must use CSPs that have an ATO granted by the FedRAMP Joint Authorization Board or another agency.²⁰ If the CSP or their offering is not FedRAMP authorized, the component must submit a request to the DOJ CIO, who will initiate the FedRAMP sponsorship process. Components must complete the security and privacy control assessments in accordance with the *DOJ SPAA Handbook* and obtain an ATO before operations.

All component-specific FedRAMP assessment information must be entered by the component into DOJ's JCAM application. In addition, all CSPs must comply with the DOJ's TIC requirements, either using JCOTS or an OCIO-approved TIC solution. DOJ requires using the JAR and DOJ acquisition directives in all solicitations, including those for cloud services.

¹⁹ The NIST definition of cloud computing sets forth five essential characteristics a system must have to qualify as a Cloud System; (1) on-demand self-service, (2) broad network access, (3) resource pooling, (4) rapid elasticity or expansion, and (5) measured service.

²⁰ https://www.fedramp.gov/assets/resources/documents/FedRAMP_Policy_Memo.pdf.

F. Protection of Mobile Devices and Removable Media

Information physically transported outside the DOJ's secured physical perimeter is more vulnerable to compromise. Accordingly, information on mobile devices and removable media must be encrypted using a FIPS-validated or an NSA-approved encryption mechanism, based on the classification of information processed on the device, unless the data is determined, in writing, to be non-sensitive by the Head of Component or designee. Laptop computers must use antivirus software and a host-based firewall mechanism. Components must ensure all security-related updates are installed on mobile computers and devices.

Mobile devices that are not in compliance with DOJ's security requirements will be subject to disconnection based upon an assessment of risk to DOJ information and operations. Components shall review and approve all applications installed on mobile devices (*i.e.*, allow listing).²¹ Information on mobile devices categorized as "federal record information" must be managed by the component in accordance with applicable records retention schedules and departmental and component policies on collection and retention of the information.

G. External Information Systems

Connections to networks external to DOJ that support access to DOJ-hosted resources must be obtained through JCOTS or a DOJ OCIO-approved TIC solution unless the DOJ CIO grants a waiver based upon assessed risk, mitigation controls, and operational requirements. Components must ensure all external information system connections are documented, assessed, and approved in accordance with the *DOJ SPAA Handbook*.

H. Wireless Communication Platforms

DOJ wireless communication platforms are information systems subject to this Order's authorities, policies, and procedures. Wireless communication platforms include all Land-Mobile Radio Systems, Unmanned Aircraft Systems (UAS), Counter-UAS systems, and unmanned ground vehicles that are capable of processing, storing, or transmitting the information. Component heads shall ensure that all wireless communication platforms follow the IT acquisition review and supply chain assessment processes, regardless of intended purpose or dollar value. In addition, components shall identify all wireless communications platforms and ensure the inventory is maintained and associated with an information system boundary in JCAM.

²¹ See the *DOJ Mobile Device and Mobile Application Security Plan*.

III. Roles and Responsibilities

The following roles are accountable for overseeing the effectiveness of the Department's security posture and protection of information resources necessary to support the DOJ's mission and operations. The responsibilities outlined below must be carried out to comply with FISMA requirements.

A. DOJ Chief Information Officer

The Deputy Assistant Attorney General, Information Resources Management (DAAG/IRM), serves as the DOJ CIO. The DOJ CIO advises and assists the Attorney General (AG), the Deputy AG (DAG), the Assistant Attorney General for Administration (AAG/A), and other senior staff to ensure that DOJ plans, acquires, manages, secures, and uses IT in a manner that enhances mission accomplishment, improves work processes and paperwork reduction, provides sufficient protection for the privacy of personal information, and is consistent with applicable federal laws, regulations, and guidance. These functions are inherently governmental and therefore must only be assigned to government personnel. In addition to the responsibilities outlined in DOJ Order 0903, *Information Technology Management*, the DOJ CIO's responsibilities include:

1. Developing, implementing, and managing a DOJ-wide POA&M process to correct cybersecurity weaknesses;
2. Reviewing, approving, and overseeing all IT acquisitions in accordance with the *Federal Information Technology Acquisition Reform Act*;
3. Ensuring that senior agency officials provide cybersecurity protections commensurate with the potential risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or damage or destruction of (a) information collected or maintained by or on behalf of DOJ, and (b) information systems used or operated by an agency, a contractor of an agency, or another organization on behalf of an agency;
4. Enforcing this Cybersecurity Program, including exercising all authorities of the CIO under FITARA levying sanctions on components for non-compliance;
5. Developing and maintaining a central repository of information on new and emerging technologies;
6. Coordinating the evaluations of new and emerging technologies by components;
7. Ensuring that DOJ personnel with access to DOJ networks and all individuals

at contractor facilities who work on DOJ systems or information, or provide services, receive and complete annual cybersecurity awareness training;

8. Ensuring cybersecurity management processes are integrated with DOJ or component strategic and operational planning processes;
9. Concurring with or disapproving waiver requests that are related to non-U.S. citizens who may access or assist in the development, operation, management, or maintenance of DOJ information systems;
10. Approving and monitoring waivers to cybersecurity requirements (other than waivers relating to non-U.S. citizens who may access or assist in the development, operation, management, or maintenance of DOJ information systems);
11. Approving encryption technologies that are not FIPS-validated in those situations where FIPS-validated products are not available;
12. Appointing a CISO to carry out the DOJ-wide cybersecurity program, as required by FISMA;
13. Taking appropriate action if a component, contractor, or other non-DOJ organization or its representative is found to be non-compliant with DOJ cybersecurity policies;
14. Establishing a Cybersecurity Committee under the DOJ CIO Council²² with supporting project teams composed of lead-component cybersecurity personnel, which shall advise the CIO on cybersecurity matters; and
15. Reporting to the AG, DAG, AAG/A, and OMB on the DOJ's Cybersecurity Program status.

The DOJ CIO may designate any cybersecurity-related responsibilities to be carried out by the DOJ CISO.

B. DOJ Chief Information Security Officer

The DOJ CISO is responsible for managing and overseeing the DOJ Cybersecurity Program and its associated activities, including those designated by the DOJ CIO. The CISO chairs DOJ's Cybersecurity Committee, established by the DOJ CIO Council. Additionally, the CISO is the principal lead for DOJ to implement FISMA requirements. These functions are inherently governmental and therefore must only be assigned to government personnel. The CISO also serves as the DOJ CIO's

²² DOJ Order 0903, *Information Technology Management*.

liaison to federal agencies for all matters related to implementing information system security and DOJ's Cybersecurity Program. The DOJ CISO's responsibilities include:

1. Developing standards and guidelines for conducting risk assessments to assess risk and determine needs;
2. Developing, implementing, and maintaining DOJ-wide cybersecurity policies and procedures for related controls to cost-effectively reduce risks to an acceptable level;
3. Monitoring, evaluating, and periodically testing information system security and privacy controls and techniques to ensure that they are effectively implemented;
4. Developing and maintaining a DOJ-wide Cybersecurity Program;
5. Providing leadership to the Cybersecurity Committee in its guidance on the management and implementation of DOJ's Cybersecurity Program;
6. Identifying and developing common security and privacy controls and managing the implementation and assessment of those controls;
7. Reviewing and approving DOJ system contingency plans and test results;
8. Ensuring and promoting a comprehensive information system security training program for both privileged and general users;
9. Assessing waiver requests for DOJ's cybersecurity standards on behalf of the CIO;
10. Preparing the annual and quarterly FISMA reports for the DOJ CIO;
11. Ensuring compliance with monthly reporting on the effectiveness of component cybersecurity programs, including the progress of remedial actions;
12. Identifying information system security management and reporting tools through the Cybersecurity Committee for use throughout DOJ;
13. Assisting senior DOJ component information system security officials with their responsibilities through the Cybersecurity Committee; and
14. Reporting to the DOJ CIO at least quarterly, in accordance with guidance issued by the DOJ CIO, on the status of compliance with the Cybersecurity Program.

C. Department Security Officer

The DSO conducts security compliance reviews to assess the overall effectiveness of security program implementation, including cybersecurity across DOJ. This function has inherent U.S. Government authority and must only be assigned to government personnel. The DSO ensures that cybersecurity reviews that require system testing are coordinated with the DOJ CIO, and all cybersecurity-related findings are reported to the DOJ CIO. The DSO's responsibilities include:

1. Advising the DOJ CIO on security program areas affecting IT;
2. Concurring with or disapproving requests for waivers related to non-U.S. citizens who may access or assist in the development, operation, management, or maintenance of DOJ information systems; and
3. Ensuring the development and implementation of DOJ-wide policy and procedures to govern emissions security, technical surveillance countermeasures monitoring, personnel security, physical and environmental security, data storage and classification marking, media disposal, media reuse, communications security materials, facsimile security, and copier security, as well as directly ensuring personnel security, document security, physical security, communications security, and emergency planning described in DOJ Order 0903, *Information Technology Management*.

D. Head of Component or Designee(s)

The Head of Component, or designated component CIO or equivalent, must establish and maintain a component-wide Cybersecurity Program to secure the component's information systems, networks, and data in accordance with DOJ policy, procedures, and guidance. These functions are inherently governmental and may be assigned or delegated to government personnel only. The Head of Component, or designee(s), works with the DOJ CISO through the Cybersecurity Committee to carry out the following responsibilities at the component level:

1. Implementing DOJ policy, standards, and guidelines;
2. Implementing the DOJ's Cybersecurity Program at the component and system levels and reporting results in accordance with OCIO guidelines;
3. Developing and implementing a component-level cybersecurity program;
4. Ensuring that monitoring, testing, and evaluating the effectiveness of cybersecurity policy, procedures, practices, and security and privacy controls, which are to be performed with a frequency depending on risk, are completed

as directed by CSS;

5. Ensuring the completion of periodic assessments of risk, including the magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or damage or destruction of information and information systems that support DOJ's operations and assets;
6. Developing, implementing, managing, and prioritizing corrective POA&Ms to correct known weaknesses in cybersecurity using the DOJ-wide POA&M process;
7. Reporting quarterly to the DOJ CIO and CISO, in accordance with guidance issued by the JMD or the DOJ CIO, on the status of the component cybersecurity program;
8. Integrating security and privacy in the Capital Planning and Investment Control process;
9. Ensuring that roles and responsibilities within the component are assigned (*e.g.*, component Cybersecurity Committee member, component CIO, AO, SCOP, Certification Agent, information system owner, information owner, user representative, and Information System Security Officer);
10. Coordinating with the DOJ OCIO on any evaluations of new technologies that could impact the DOJ's enterprise security architecture;
11. Participating with other components and the DOJ OCIO in evaluating and selecting cybersecurity tools for use within DOJ and obtaining DOJ CIO approval for non-enterprise cybersecurity solutions;
12. Establishing procedures to ensure that software installed on component information systems is in compliance with applicable copyright laws and is incorporated into the information system's life cycle management process;
13. Approving, with the concurrence of the DOJ CIO and DSO, waivers related to non-U.S. citizens who may access or assist in the development, operation, management, or maintenance of DOJ information systems and monitoring these waivers;
14. Ensuring that all component personnel with access to DOJ networks and all individuals at contractor facilities who work on DOJ systems or information or provide services receive and complete annual cybersecurity awareness training; and
15. In coordination with the DOJ CIO and CPCLO, identifying and planning

for the resources needed to implement information security and privacy programs, including ensuring that investment plans submitted to OMB as part of the budget process meet information security and privacy requirements.²³

E. Chief Privacy and Civil Liberties Officer

The CPCLO serves as DOJ's official with primary responsibility for DOJ's privacy policy. The CPCLO determines the DOJ's privacy policy and standards, consistent with applicable law, regulation, and administration policy and in consideration of the Fair Information Practice Principles. The CPCLO is the principal advisor to DOJ leadership and components on privacy and civil liberties matters affecting DOJ's mission and operations.

The CPCLO serves as DOJ's Senior Agency Official for Privacy and oversees DOJ's privacy and civil liberties programs and initiatives implemented by the OPCL, DOJ components, and component privacy and civil liberties officials. In addition to the responsibilities outlined in DOJ Order 0601, *Privacy and Civil Liberties* (or its successor order), the CPCLO is responsible for:

1. Ensuring close coordination between DOJ's privacy personnel and the DOJ CIO, CISO, component CIOs, and other DOJ cybersecurity officers, as appropriate;
2. Ensuring DOJ resource planning and management activities consider privacy throughout the SDLC and that the risks are appropriately managed;
3. Incorporating federal privacy requirements into DOJ's enterprise architecture to ensure that risk is addressed, and information systems achieve the necessary levels of trustworthiness, protection, and resilience;
4. Reviewing IT capital investment plans and budgetary requests in consultation with component heads to help ensure that privacy requirements (and associated privacy controls), as well as any associated costs, are explicitly identified and included, with respect to any IT resources that will be used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII;
5. Reviewing and approving in accordance with NIST FIPS 199 and SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, the categorization of information systems that create,

²³ See also DOJ Order 0601, *Privacy and Civil Liberties* (requiring CPCLO to analyze IT investment plans and budget requests; requiring component head to consult with CPCLO when considering new information systems or technologies and ensuring compliance with legal obligations; and requiring sufficient support, training, and resources for SCOPs to complete their duties effectively).

collect, use, process, store, maintain, disseminate, disclose, or dispose of PII;

6. Designating which privacy controls will be treated as program management, common, information system-specific, and hybrid privacy controls;
7. Reviewing and approving the privacy plans for DOJ information systems before authorization, reauthorization, or ongoing authorization;
8. Identifying assessment methodologies and metrics to determine whether privacy controls are: (a) implemented correctly, (b) operating as intended, and (c) sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks;
9. Conducting and documenting the results of privacy control assessments to (a) verify the continued effectiveness of all privacy controls selected and implemented at the agency across all agency risk management tiers to ensure continued compliance with applicable privacy requirements and (b) manage privacy risks;
10. Developing and maintaining a privacy continuous monitoring strategy;
11. Establishing and maintaining a privacy continuous monitoring program that implements DOJ's privacy continuous monitoring strategy and maintains ongoing awareness of threats and vulnerabilities that may pose privacy risks; monitors changes to information systems and environments of operation that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII; and conducts privacy control assessments to (a) verify the continued effectiveness of all privacy controls selected and implemented at the agency across the agency risk management tiers to ensure continued compliance with applicable privacy requirements; and (b) appropriately manage privacy risks;
12. Reviewing authorization packages for information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII to ensure compliance with applicable privacy requirements and manage privacy risks before AOs make risk determination and acceptance decisions; and
13. Ensuring that DOJ considers appropriate privacy protections in the collection, storage, use, disclosure, and security of PII, with respect to DOJ's existing or proposed IT and information systems.

The CPCLO has the authority to delegate the responsibilities listed above to appropriate officials within the Department, including the OPCL Director, the DOJ

CIO, the DOJ CISO, or any designated component official including Heads of Components, or the applicable SCOP, so long as such delegation is consistent with federal law and DOJ policy and subject to the CPCLO's oversight and control.

APPENDIX A: AUTHORITIES

Federal Statutes
Privacy Act of 1974 (Public Law 93-579)
Government Performance and Results Act of 1993 (Public Law 103-62)
Clinger-Cohen Act of 1996 (Public Law 104-106)
Workforce Investment Act of 1998; Title IV, Rehabilitation Act Amendments, Section 508 (Public Law 105-220)
Government Paperwork Elimination Act of 1998 (Public Law 105-277)
Electronic Signatures in Global and National Commerce Act of 2001 (Public Law 106-229)
Homeland Security Act of 2002 (Public Law 107-296)
E-Government Act of 2002 (Public Law 107-398), which includes the Federal Information Security Management Act
Government Performance and Results Modernization Act of 2011 (Public Law 111-325)
Federal Information Security Modernization Act of 2014 (Public Law 113-283)
Federal Information Technology Acquisition Reform Act of 2014 (Public Law 113-291)

Office of Management and Budget Circulars
OMB Circular A-11: Preparing, Submitting, and Executing the Budget, August 2021
OMB Circular A-76: Performance of Commercial Activities, August 1983
OMB Circular A-94: Discount Rates to be Used in Cost-Benefit Analysis, October 1992
OMB Circular A-130: Managing Information as a Strategic Resource, July 28, 2016

Orders Office of Management and Budget and Agency Memoranda
M-03-22: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (September 26, 2003)
M-04-26: Personal Use Policies and File Sharing Technology, September 2004
M-05-08: Designation of Senior Agency Officials for Privacy (February 11, 2005)
M-05-23: Improving Information Technology Project Planning and Execution, August 2005
M-05-24: Implementation of Homeland Security Presidential Directive (HSPD-12) Policy for a Common Identification Standard for Federal Employees/Contractors, August 2005
M-06-02: Improving Public Access to and Dissemination of Government Information and Using the Federal Enterprise Architecture Data Reference Model, December 2005
M-06-15: Safeguarding Personally Identifiable Information, May 2006
M-09-02: Information Technology Management Structure and Governance Framework, October 2008
M-10-22: Guidance for Online Use of Web Measurement and Customization Technologies, June 2010
M-10-23: Guidance for Agency Use of Third-Party Websites and Applications, June 2010
M-10-25: Reforming the Federal Government's Efforts to Manage Information Technology Projects, June 2010

M-10-26: Immediate Review of Financial Systems IT Projects June 2010

Presidential Orders and Office of Management and Budget and Agency Memoranda

M-10-27: IT Investment Baseline Management Policy, June 2010

M-10-28, Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security, July 2010

M-10-31: Immediate Review of IT Projects, July 2010

M-10-32: Evaluating Programs for Efficacy and Cost Efficiency, July 2010

M-11-02: Sharing Data While Protecting Privacy

M-11-29: Chief Information Officer Authorities, August 2011

M-12-10: Implementing Portfolio Stat, March 31, 2012

M-13-13, Open Data Policy – Managing Information as an Asset, May 9, 2013

M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government October 30, 2015

M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017)

M-19-03, Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program, December 10, 2018

M-19-26, Update to the Trusted Internet Connections (TIC) Initiative, September 12, 2019

M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management, May 21, 2019

M-21-04, Modernizing Access to and Consent for Disclosure of Records Subject to the Privacy Act, November 12, 2020

M-21-07, Completing the Transition to Internet Protocol Version 6 (IPv6), November 19, 2020

M-21-30, Protecting Critical Software Through Enhanced Security Measures, August 10, 2021

M-21-31, Improving the Federal Government’s Investigative and Remediation Capabilities Related to Cybersecurity Incident, August 27, 2021

M-22-01, Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response, October 8, 2021

M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, January 26, 2022

M-22-05, Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements (December 6, 2021)

Executive Order 14028: Improving the Nation’s Cybersecurity, May 2021.

Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems, January 19, 2022

DOJ Orders, Policy Statements, and Instructions

DOJ Order 2422.1A, Radio Communications Policy, Responsibilities, Standards, and Procedures, August 9, 2002

DOJ Instruction 0900.00.01, Incident Response Procedures for Data Breaches, August 6, 2013

DOJ Orders, Policy Statements, and Instructions
DOJ Policy Statement 0900.01, Data Center Facilities Enhancement and Relocation of Information Technology Infrastructure, November 14, 2013
DOJ Order 0901, Insider Threat, February 12, 2014
DOJ Order 0601, Privacy and Civil Liberties, May 14, 2020
DOJ Order 0801.04, Electronic Mail Records Retention, May 8, 2015
DOJ Order 0902, Accessible Electronics and Information Technology, October 15, 2015
DOJ Order 0903, Information Technology Management, May 5, 2016
DOJ Order 0908, Use and Monitoring of DOJ Information Technology, Information Systems, and Access to an Authorized Users' Electronic Information, September 15, 2016
DOJ Policy Statement 0904.01, Identify, Credential, and Access Management, September 14, 2020
DOJ Policy Statement 0904.02, Incident and Breach Response Playbook

Federal and Departmental Regulations/Guidance
DOJ Strong Authentication Plan
DOJ Mobile Device and Mobile Application Security Plan
DOJ Security Assessment and Privacy Assessment and Authorization Handbook
DOJ Incident Response Plan
DOJ Configuration Management Plan
DOJ Supply Chain Risk Management Plan
Committee on National Security Systems Instruction No. 1253: Security Categorization and Control Selection for National Security Systems
Department of Homeland Security Trusted Internet Connections (TIC) 3.0 Reference Architecture Volume 2, v1.1, July 2021
Intelligence Community Directive 503: Intelligence Community Information Technology Systems Security Risk Management
NIST FIPS 199: Standards for Security Categorization of Federal Information and Information Systems
NIST SP 800-12 Revision 1: An Introduction to Computer Security
NIST SP 800-30: Revision 1: Guide for Conducting Risk Assessments
NIST SP 800-37 Revision 2: Risk Management Framework for Information Systems and Organizations
NIST SP 800-39: Managing Information Security Risk: Organization, Mission, and Information System View
NIST SP 800-53 Revision 5: Security and Privacy Controls for Federal Information Systems and Organizations
NIST SP 800-53A Revision 5: Assessing Security and Privacy Controls in Federal Information Systems and Organizations
NIST SP 800-59: Guide for Identifying an Information System as a National Security System
NIST SP 800-60: Guide for Mapping Types of Information and Information Systems to Security Categorization Levels

Federal/Departmental Regulations/Guidance

NIST SP 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

NIST SP 800-161: Supply Chain Risk Management Practice for Federal Information Systems and Organizations

NIST Interagency or Internal Report (IR) 8286: Integrating Cybersecurity and Enterprise Risk Management

United States Government Accountability Office (GAO): Information Technology: A Framework for Assessing and Improving Enterprise Architecture Management v2.0, GAO-10-846G, August 2010