



Approved On:

DOJ Order

SEP 15 2016

CYBERSECURITY PROGRAM

PURPOSE: Maintains and enhances the Department of Justice (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 information; contractors and other users 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 technology (IT) resources, such as other federal agencies; IT systems that process national security information and unclassified information

ORIGINATOR: Justice Management Division, 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; Office of Management and Budget Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016

CANCELLATION: DOJ Order 2640.2F

DISTRIBUTION: Electronically distributed to those referenced in the "SCOPE" section and posted to the DOJ directives electronic repository (SharePoint) at: <https://portal.doj.gov/sites/dm/dm/Pages/Home.aspx>

APPROVED BY: *Lee J. Lofthus*
Assistant Attorney General for Administration 

ACTION LOG

DOJ directives are reviewed, at minimum, every 5 years and revisions are made as necessary. The action log records dates of approval, recertification, and cancellation, as well as major and minor revisions to this directive. A brief summary of revisions will be noted. In the event this directive is cancelled, superseded, or supersedes another directive, that will also be noted in the action log.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	Reflects updated security requirements for DOJ information and information systems.

TABLE OF CONTENTS

ACTION LOG	2
DEFINITIONS.....	5
ACRONYMS.....	9
I. Policy	11
A. Serves as the Central Focal Point for Cybersecurity.....	11
B. Deploys and Manages a Department-wide Common Security Strategy.....	11
C. Identifies New and Emerging Technologies	12
D. Develops Cybersecurity Policy, Procedures, and Templates.....	12
E. Promotes Awareness of Security Risks and Policies	12
F. Develops Standards for, and Performs, Security and Privacy Control Monitoring and Evaluation	12
G. Develops and Manages a Comprehensive Risk Management Program.....	13
H. Identifies and Documents Information Systems	13
I. Protects the Privacy of Individuals.....	13
II. Information System Security and Privacy Requirements	14
A. Security Control Families.....	14
B. Privacy Control Families and Additional Privacy Requirements	23
C. Contractor Access to Information Systems.....	26
D. Use of DOJ IT Resources Outside the United States.....	27
E. Classified Information.....	28
F. Cloud Computing.....	29
G. Protection of Mobile Devices and Removable Media	29
H. External Information Systems.....	30
III. Implementing the Risk Management Framework for DOJ Systems	31
A. Categorize Information Systems	31
B. Select Security and Privacy Controls.....	32
C. Implement Security and Privacy Controls	32
D. Assess Security and Privacy Controls.....	33
E. Authorize Information System.....	33
F. Monitor Security and Privacy Controls.....	33
IV. Roles and Responsibilities	34
A. DOJ Chief Information Officer	34
B. DOJ Chief Information Security Officer.....	36
C. Department Security Officer	37

D. Head of Component or Designee(s) 38
E. Chief Privacy and Civil Liberties Officer 39
APPENDIX: AUTHORITIES 42

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., nonlocal 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 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
Authority to Operate	The official management decision given by an Authorizing Official or other designated senior DOJ official to authorize 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 the 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.
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 National Institute of Standards and Technology SP 800-145.
Continuous Monitoring	Maintaining ongoing awareness to support organizational risk decisions.
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.
Data	A subset of information in an electronic format that allows it to be retrieved or transmitted.
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.
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 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, without limitation, information related to DOJ programs or personnel. It includes, without limitation, information (1) provided by, generated

Term	Definition
	by, or generated for DOJ, (2) provided to DOJ and in DOJ custody, and/or (3) managed or acquired by a DOJ contractor in connection with the performance of a contract.
Information system	A discrete set of information resources organized for collecting, processing, maintaining, using, sharing, disseminating, or disposing of information. Information system includes specialized systems such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.
Information System Security Officer	An individual with assigned responsibility for maintaining the appropriate operational security level for an information system or program.
National security information	Information that has been determined (pursuant to Executive Order 12958 as amended by Executive Order 13292, or any successor order, or by the Atomic Energy Act of 1954, as amended) to require protection against unauthorized disclosure and is marked to indicate its classified status.
Personally identifiable information	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.
Privacy Continuous Monitoring Strategy	A formal document that catalogs the available 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 privacy requirements and to manage privacy risks.
Privacy Plan	A formal document that (1) details the privacy controls selected for an information system or environment of operation that are in place, or planned, for meeting applicable privacy requirements and managing privacy risks; (2) details how the controls have been implemented; and (3) describes the methodologies and metrics that will be used to assess the controls. The Privacy Plan and the Security Plan may be integrated into one consolidated document.
Risk	The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals, resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

Term	Definition
Risk management	The process of managing risks to DOJ operations (including mission, functions, image, 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.
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 through the use of dedicated connections, virtual tunneling protocols, or traffic encryption.

ACRONYMS

Acronym	Meaning
AAG/A	Assistant Attorney General for Administration
AG	Attorney General
AO	Authorizing Official
ATO	Authority to Operate
CD	Compact disc
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNSS	Committee on National Security Systems
CPCLO	Chief Privacy and Civil Liberties Officer
CSAM	Cyber Security Assessment and Management
CSP	Cloud service provider
CSS	Cybersecurity Services Staff
DAAG/IRM	Deputy Assistant Attorney General/Information Resources Management
DAG	Deputy Attorney General
DHCP	Dynamic Host Configuration Protocol
DNI	Director of National Intelligence
DNS	Domain name system
DOJ	Department of Justice
DSO	Department Security Officer
DVD	Digital video disc
FedRAMP	Federal Risk and Authorization Management Program
FIPP	Fair Information Practice Principles
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
GAO	Government Accountability Office
HTTPS	Hypertext Transfer Protocol Secure
ICD	Intelligence Community Directive
IT	Information technology

Acronym	Meaning
JSOC	Justice Security Operations Center
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSI	National security information
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
OPCL	Office of Privacy and Civil Liberties
PGD	Procurement Guidance Document
PII	Personally identifiable information
POA&M	Plan of Action and Milestones
SAOP	Senior Agency Official for Privacy
SCI	Sensitive compartmented information
SCOP	Senior Component Official for Privacy
SDLC	Systems development lifecycle
SP	Special publication
SPE	Senior Procurement Executive
SPOM	Security Program Operating Manual
SSPP	System Security and Privacy Plan
TIC	Trusted Internet connection
TICAP	Trusted Internet connection access provider
USB	Universal serial bus
VPN	Virtual private network
US-CERT	United States Computer Emergency Readiness Team

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 (Department or DOJ) to maintain a DOJ-wide Cybersecurity Program that collaboratively maximizes resources; protects DOJ information systems and operations; and establishes the governance framework, policy requirements, and standards for managing the security and privacy of departmental electronic information 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 develop and implement its mission to protect itself against malicious attempts to damage, disrupt, or gain unauthorized access to its information systems. The DOJ Chief Information Security Officer (CISO) manages and oversees the Cybersecurity Program, which performs the following functions:

A. Serves as the Central Focal Point for Cybersecurity

The Cybersecurity Services Staff (CSS) serves as the central focal point for cybersecurity in DOJ. CSS provides DOJ-wide management and implementation of the DOJ Cybersecurity Program. CSS and the components provide a collaborative team to manage the accomplishment of priorities for achieving business objectives and complying with the required rules and regulations including, but not limited to, those listed in Appendix A, such as FISMA; Homeland Security Presidential 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; Director of National Intelligence (DNI) directives; and DOJ cybersecurity requirements.

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

DOJ follows a common security strategy that defines security goals for the components. These goals outline DOJ's security posture, both internally and externally, while taking into account the respective business needs and missions of each component. DOJ's common security strategy is strengthened by the adoption of a common information system security architecture developed to ensure that information technology (IT) systems remain secure throughout their entire lifecycle. Security needs and requirements must be identified at the beginning of the systems development lifecycle (SDLC) and funded appropriately.

C. Identifies New and Emerging Technologies

Technology is a dynamic field with new and emerging technologies constantly being identified that could assist DOJ with accomplishing its evolving mission better. The DOJ Office of the Chief Information Officer (OCIO) must provide a central repository of information on these technologies. Components must coordinate with the OCIO prior to undertaking any evaluation of new or emerging technologies that will or may be connected to a DOJ network or system.

D. Develops Cybersecurity Policy, Procedures, and Templates

DOJ's cybersecurity policies must clearly address DOJ's information system security and privacy needs and serve as the foundation for DOJ's Cybersecurity Program. Policy must represent the primary mechanism for senior management to communicate its cybersecurity requirements to the components. Policy will be revised as required and will be related to the risk of DOJ or components not being able to perform their functions.

DOJ's cybersecurity standards must provide detailed and practical procedures for implementing DOJ policy. These standards must outline specific requirements for accomplishing DOJ's cybersecurity goals.

E. Promotes Awareness of Security Risks and Policies

DOJ information systems users must be continually educated on security risks and related policy, as they are more likely to support and comply with the policy if they understand the purpose behind the policy and their own associated responsibilities. CSS will continually work with components to educate and provide resources to promote awareness to users.

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

DOJ's cybersecurity and privacy programs must be monitored and assessed continually against cybersecurity and privacy policies and controls to ensure the policies and controls remain appropriate and effective. Monitoring control effectiveness and compliance with policy must be incorporated within the cycle of managing the DOJ's cybersecurity and privacy programs, incorporating the use of automated software tools when possible.

G. Develops and Manages a Comprehensive Risk Management Program

DOJ and component senior management must develop and manage information systems based on a thorough examination of the risks identified in assessments and the impact the information system has on DOJ operations. Additionally, the risk management strategy must be continually evaluated to ensure it addresses the current threats to DOJ information systems.

This risk management strategy is based on the concepts found in the OMB Circular A-130, FISMA, the NIST Risk Management Framework, NIST Special Publication (SP) 800-37 and other federal guidance. It presents a formal, structured approach for developing risk assessments for information systems and provides a uniform standard for evaluating security and privacy risks to information systems operating within DOJ. The primary focus of this methodology must be on the information system's mission, not on the specific IT asset. Since risk management is an essential management function, DOJ information system owners and cybersecurity managers must use this methodology when assessing risks and prioritizing resources for the security assessment and authorization of DOJ information systems and incorporate system risk management into the larger scope of enterprise risk management.

H. Identifies and Documents Information Systems

Components must identify and document each information system, and DOJ information may only be processed, stored, or transmitted on information systems that meet the requirements contained in this Order.

I. Protects the Privacy of Individuals

While security and privacy are independent and separate disciplines, they are closely related and, therefore, it is essential for DOJ to take a coordinated approach to identifying and managing security and privacy risks and complying with security and privacy requirements. 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.

In implementing the Cybersecurity Program, components, and DOJ as a whole, must ensure that privacy needs and requirements are identified at the beginning of the SDLC and are funded appropriately; that DOJ's Risk Management Framework fully integrates DOJ's privacy program requirements, including the selection, implementation, and assessment of privacy controls; and that the DOJ Chief Information Officer (CIO), DOJ CISO, and cybersecurity personnel coordinate with the CPCLO, OPCL, and DOJ's privacy personnel.

II. Information System Security and Privacy Requirements

A. Security Control Families

The DOJ cybersecurity standard requires components to undertake specific actions at prescribed intervals to implement and manage the implementation of security and privacy requirements.

Security controls are designed to be technology neutral such that the focus is on the fundamental countermeasures needed to protect DOJ information and information systems.

1. Access Control

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

a. 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 devices (including other information systems) and to the types of transactions and functions authorized users are permitted to exercise.
- Prohibit automatic forwarding of email received in DOJ email systems to or through a non-DOJ email system, unless the Authorizing Official (AO) grants a waiver.
- 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 unless a request for a waiver has been submitted by the Head of Component to, and approved by, the DOJ CIO and the DOJ Security Officer (DSO).

b. Remote access

Remote access is any access to non-public DOJ information systems by a DOJ employee or contractor communicating through an external, non-DOJ-controlled network.

- For general user access, components must restrict remote access to non-public DOJ information systems to government-authorized devices using an encrypted virtual private network (VPN) to connect to DOJ information systems, unless otherwise approved by the information system AO. For devices not government-authorized, components must follow the guidance in the *DOJ Strong Authentication Plan*.
- For privileged user access, components must restrict remote access to government-authorized devices using an encrypted VPN to connect to DOJ information systems.
- For “a” and “b” above, components must not allow users to connect remote-access devices to any other network when those devices are connected to a DOJ information system.

c. Public access

Public access is the access provided to non-DOJ users to public facing or publicly accessible DOJ information systems.

- For publicly accessible DOJ information systems without identification and authentication requirements, access must be open, unless access for certain users or groups should be restricted for cybersecurity or performance reasons.
- For public facing DOJ information systems containing non-public DOJ information accessible by DOJ employees and contractors as well as non-DOJ personnel, components must restrict access to authenticated users with validated requirements.

2. Audit and Accountability

DOJ information systems must:

- a. Create, protect, and retain information system audit records to the extent needed to enable security monitoring, analyzing, investigating, and reporting of unlawful, unauthorized, or inappropriate information system activity;

- b. Ensure that actions of authenticated information system users can be uniquely traced to those users so that they can be held accountable for their actions; and
- c. Provide direct, real-time or near real-time electronic data feeds, as applicable, of all relevant security monitoring and auditing data to the Justice Security Operations Center (JSOC) systems unless the DOJ CIO grants a waiver based upon assessed risk, mitigating controls, and operation requirements. (Examples include but are not limited to firewall event logs, intrusion detection or prevention system alerts and logs, and network and desktop antivirus event logs).

3. Awareness and Training

Components must:

- a. Ensure that managers and users of DOJ information systems are aware of the security risks associated with their activities and of the applicable laws, regulations, directives, policies, standards, instructions, and procedures related to the security of DOJ information systems and data, including digital and paper systems and data; and
- b. Provide component personnel with training to carry out their assigned information system security-related duties and responsibilities.

4. Configuration Management

In accordance with the *DOJ Configuration Management Plan*, components must:

- a. Establish and maintain baseline configurations and inventories of DOJ information systems (including hardware, software, firmware, and documentation) throughout the respective SDLCs;
- b. Establish a configuration change control process to ensure proposed changes are evaluated, tested, approved, and documented properly before being put into production; and
- c. Establish and enforce security settings consistent with the information system operational requirements and validate those controls through DOJ-approved tools.

5. Contingency Planning

Components must establish, maintain, and effectively implement plans for emergency response, 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. These plans and actions must be tested and exercised in accordance with the latest iteration of the *DOJ Information System Contingency Planning Guide*.

6. Identification and Authentication

DOJ information systems must:

- a. Identify information system users, processes acting on behalf of users, and/or devices;
- b. Authenticate (or verify) the identities of those users, processes, and/or devices prior to granting them access to DOJ information systems (this does not apply to unauthenticated access to public information systems); and
- c. Require users to authenticate to DOJ information systems in accordance with the *DOJ Strong Authentication Plan*.

7. Incident Response

Components must:

- a. Establish an operational incident handling capability for DOJ information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities in coordination with the JSOC;
- b. Track, document, and report security incidents to appropriate DOJ officials and/or authorities;
- c. Notify the JSOC within 1 hour of a suspected cybersecurity incident when the confidentiality, integrity, or availability of a Federal Government information system is threatened (the JSOC is responsible for reporting confirmed incidents within 1 hour to the United States Computer Emergency Readiness Team (US-CERT) as defined by the US-CERT guidance);
- d. Provide DOJ forensics and law enforcement personnel, including the Inspector General (IG), access to media and devices required for investigation, when appropriate;

- e. Assist with digital forensic and other investigations on electronic devices and/or associated media, when requested and appropriate; and
- f. Maintain a chain of custody to record the handling and transfer of media and devices to support forensic and other investigations.

8. Maintenance

Components must:

- a. Perform periodic and timely maintenance on DOJ information systems; and
- b. Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct on-site and remote information system maintenance.

9. Media Protection

Components must:

- a. Protect information system media in all forms;
- b. Use a previously authorized component file sharing solution or the DOJ Enterprise File Sharing solution for the sharing of information;
- c. Encrypt sensitive and classified information transported or “at-rest” outside the agency’s secured, physical perimeter in digital format using Federal Information Processing Standards (FIPS) 140-2 validated or National Security Agency (NSA) approved encryption, as appropriate. 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;
- d. Limit access to DOJ information systems and DOJ information to authorized users;
- e. Sanitize or destroy information system media before disposal or release for reuse in accordance with *DOJ Security Program Operating Manual (SPOM)*, Annex G, “Sanitizing and Releasing Computer Components”; and

- f. 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.

10. Personnel Security

Non-U.S citizens are not 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 a request for a waiver has been submitted by the Head of Component to, and approved by, the DOJ CIO and the DSO allowing access or assistance by the non-U.S. citizen.

Components must:

- a. 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;
- b. 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 a request for a waiver has been submitted by the Head of Component to, and approved by, the DOJ CIO and the DSO specifically allowing access or assistance by the non-U.S. citizen;
- c. Ensure that DOJ information and information systems are protected during and after personnel actions, such as a termination and transfer; and
- d. Employ formal sanctions for personnel failing to comply with DOJ security policy and procedures, in accordance with applicable laws and regulations.

11. Physical and Environmental Protection

Components must perform the following for an internally hosted information system or ensure the following for an externally hosted information system:

- a. Limit physical access to information systems, equipment, and the respective operating environments to authorized individuals and monitor and log such accesses;
- b. Protect the physical facility and support infrastructure for information systems;

- c. Provide supporting utilities for information systems;
- d. Protect information systems against environmental hazards; and
- e. Provide appropriate environmental controls in facilities containing information systems.

12. Planning

Components must develop, document, update, and implement:

- a. Security plans for DOJ information systems that describe the security controls that are in place, or are planned, for the information systems; and
- b. Rules of behavior for individuals who access DOJ information systems.

13. Program Management

Components must implement a component-wide Cybersecurity Program to address cybersecurity for the information and information systems that support the operations and assets of the component, including those provided or managed by another organization, contractor, or other source.

14. Risk Assessment

Components must periodically assess the risk to departmental operations (including mission, function, image, or reputation) and assets, individuals, other organizations, and the Nation resulting from the operation of DOJ information systems and the associated processing, storing, or transmitting of DOJ information.

15. Security Assessment and Authorization

Components must:

- a. Use the Cyber Security Assessment and Management (CSAM) system or other approved system of record to record the periodic assessments of the security controls in DOJ information systems and determine if the controls are effective in their application;
- b. Develop, monitor, and implement Plans of Action and Milestones (POA&M) designed to correct deficiencies and reduce or eliminate vulnerabilities in DOJ information systems; and

- c. Authorize the operation of DOJ information systems and any associated information system interconnections prior to operational use.

16. Systems and Communications Protection

Components must perform or support the following:

- a. In accordance with the DHS *Trusted Internet Connection Reference Architecture* (as amended), components must secure all physical or logical connections between information systems, networks, or components of information systems and networks by or through the DOJ Trusted Internet Connection Access Point (TICAP) or the DOJ Cloud Security Infrastructure. (Note that this requirement to connect by or through the TICAP or DOJ Cloud Security Infrastructure does not apply to public access to public information systems without identification and authentication requirements, as noted in 16.b, below).
- b. For all publicly accessible DOJ websites and web services, components must provide service only through a secure connection and use the strongest privacy and integrity protection available for public web connections.
- c. DOJ maintains and publishes a list of known malicious resources and sites. Components must block these resources and sites at boundary protection devices. Exceptions to allow access to specific resources and/or sites on this list must be approved by the DOJ CISO and reported 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.
- d. Components must 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.
- e. Component information systems must use approved cryptographic mechanisms or protected distribution systems to protect the confidentiality and integrity of information transmitted beyond the secured physical perimeter.
- f. Components must not deploy systems, 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 prior to operational use.

17. System and Information Integrity

Components must:

- a. Identify, report, and correct information and information system flaws in accordance with the *DOJ IT Security Standard*;
- b. Provide protection from malicious code at appropriate locations within DOJ information systems; and
- c. Monitor information system security alerts and advisories and take appropriate actions in response.

18. Systems and Services Acquisition

Components must:

- a. Allocate sufficient resources to protect DOJ information systems adequately;
- b. Employ SDLC processes that incorporate information system security considerations;
- c. Ensure that new acquisitions of information systems include available commonly accepted security configurations;
- d. Perform acquisition risk assessments and develop and adopt effective supply chain risk management standards for IT acquisitions in accordance with Procurement Guidance Document (PGD) 14-03 (or its latest iteration);
- e. Employ software usage and installation restrictions to ensure that software installed on DOJ information systems complies with applicable copyright laws and licensing agreements; and
- f. 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 information, applications, and services outsourced from DOJ in accordance with PGD 15-03 (or its latest iteration).

B. Privacy Control Families and Additional Privacy Requirements

Loss or disclosure of sensitive information, such as personally identifiable information (PII), not only has a serious negative impact on DOJ's law enforcement, litigation, and other critical functions, but also diminishes the public trust in DOJ's operations. There is inherent risk in carrying such data on mobile computers and devices. Implementation of the controls in the privacy control families will ensure that the scope of DOJ's collection, use, maintenance, and dissemination of PII is limited appropriately.

The following requirements apply to DOJ programs and systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII:

1. Authority and Purpose

Components must identify the legal bases that authorize a particular PII collection or activity that impacts privacy and specify in their notices the purpose(s) for which PII is collected.

2. Accountability, Audit, and Risk Management

In an effort to enhance public confidence, components must 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.

3. Data Quality and Integrity

Components must ensure that any PII collected and maintained is accurate, relevant, timely, and complete as practicably as possible, and that it is being used for the purpose for which it was specified in public notices.

4. Data Minimization and Retention

Components must:

- a. Implement the data minimization and retention requirements to collect, use, and retain only PII that is relevant and necessary for the purpose for which it was originally collected; and
- b. Retain PII for only as long as necessary to fulfill the purpose(s) specified in public notices and in accordance with a National Archives and Records Administration-approved records retention schedule;

5. Individual Participation and Redress

Components must, when required by law, provide individuals with access to their PII and the ability to have their PII corrected or amended, as appropriate.

6. Security

Components must 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 comply with OMB policies and guidance.

7. Transparency

Components must, when required by law, provide public notice of their information practices and the privacy impact of their programs and activities.

8. Use Limitation

Components must use PII only as specified in their public notices, in a manner compatible with those specified purposes, or as otherwise permitted by law.

9. Additional Privacy Requirements

Components must:

- a. Ensure that privacy requirements and risks are addressed and appropriately managed throughout the SDLC process.
- b. 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.
- c. Consider privacy when analyzing IT investments and establish a decision-making process that must cover the life of each information system and include explicit criteria for analyzing the projected and actual costs, benefits, and risks, including privacy risks, associated with IT investments.
- d. Ensure that the component's implementation of DOJ's Risk Management Framework fully integrates the privacy requirements found within this Order,

or as otherwise required by the CPCLO, including, but not limited to, the selection, implementation, and assessment of privacy controls.

- e. Correct deficiencies that are identified through privacy assessments, the privacy continuous monitoring program, or internal or external audits and reviews.
- f. Encrypt all NIST FIPS Publication 199 moderate-impact and high-impact information at rest and in transit, unless encrypting such information is technically unfeasible or would demonstrably affect the ability of agencies to carry out their respective missions, functions, or operations, and that the risk of not encrypting is accepted by the AO and approved by the CIO, in consultation with the CPCLO, or a duly authorized official, as appropriate.
- g. Limit access to PII to those individuals who require such access;
- h. Ensure that the CPCLO, or a duly authorized official, is made aware, in a timely manner, of information systems that cannot be appropriately protected or secured and that such systems are given a high priority for upgrade, replacement, or retirement.
- i. Log all computer-readable data extracts from databases holding sensitive information and ensure that each extract including sensitive data has been erased via logical sanitization or physical destruction within 90 days or that its use is still required. All DOJ information is considered sensitive information unless designated as non-sensitive by the Head of Component.
- j. Require, as appropriate, other agencies and entities with which the component shares PII to perform the following:
 - maintain the PII in an information system with a particular NIST FIPS Publication 199 confidentiality impact level, as determined by DOJ; and
 - 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.
- k. Implement incident management and response capabilities, in accordance with law and DOJ policies. These capabilities must include requirements to notify the JSOC of incidents involving known loss of sensitive data and PII within 1

hour of discovery; establish clear roles and responsibilities to ensure the oversight and coordination of incident response activities; and ensure that incidents are documented, reported, investigated, and handled in accordance with law and DOJ policies. Loss of any data storage devices, such as laptops, flash drives, disks, and tapes, should be reported as an incident within the same 1-hour time frame (the DOJ Computer Emergency Readiness Team will notify the US-CERT and the DOJ CIO, as necessary).

- l. Ensure that the terms and conditions in contracts and other agreements involving the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of DOJ information incorporate privacy requirements and are sufficient to enable agencies to meet federal and DOJ-specific requirements pertaining to the protection of DOJ information. Such laws and DOJ policies include, but are not limited to:
 - DOJ requirements for remote access and security incident reporting;
 - Privacy Act requirements when a contractor designs, develops, or operates a system of records on behalf of DOJ to accomplish an agency function; and
 - Those requirements developed by the CPCLLO and/or DOJ's Senior Procurement Executive (SPE).
- m. Document and implement policies and procedures, consistent with this Order, for privacy oversight of contractors and other entities, to include ensuring appropriate vetting and access control processes for contractors and others with access to information systems containing DOJ information.

C. Contractor Access to Information Systems

1. Components may use contractors to design, develop, operate, and maintain information systems on their behalf. Contractors may be granted access to DOJ information systems and information in order to perform work specified under the contract. Access may be from component- or DOJ-owned computers or from contractor-owned computers. Contractors may process DOJ information on contractor-owned equipment, either within or outside DOJ space. In all of these situations, the contractors and their sub-contractors, including all personnel, information systems, and devices, are required to comply with this Order, and the contract must include the language required by PGD 15-03 (or its latest iteration), unless waived, in whole or in part, by the DOJ SPE or any other terms and conditions as deemed necessary by the CPCLLO and/or DOJ's SPE.

2. When the contract requires or allows contractor information systems to be used (whether to access DOJ information systems and information or to process or store DOJ information), the contract must require that the information systems be assessed, authorized, and operated pursuant to a valid Authority to Operate (ATO). The ATO must be issued in accordance with the ATO requirements in this document and in the *Security Assessment & Authorization Handbook* for unclassified and national security systems. Contractors who use individual devices under the contract must provide an inventory of such devices to the Contracting Officer's Representative (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.
3. Upon termination of contract work, all DOJ data must be removed from contractor-owned IT equipment. Certification of data removal must be performed by the contract's project manager and a letter confirming certification must be delivered to the contracting officer within 15 business days of the termination of the contract, unless otherwise extended by the Contracting Officer or COR.

D. Use of DOJ IT Resources Outside the United States

The DOJ CISO must approve, in writing, either individually or by blanket function, the transportation or use of DOJ desktop computers, laptop computers, and servers outside the United States. The use of DOJ mobile devices (e.g., tablet devices and smartphones) outside the United States must follow the requirements in the DOJ's *Mobile Device and Mobile Application Security Policy Instruction*. Components also must:

1. Ensure any additional approvals necessary to transport DOJ assets outside of the United States are received prior to travel;
2. Limit data taken outside the United States to that which is needed to accomplish the purpose of the travel;
3. Prevent access to DOJ information systems from outside the United States, with the exception of systems specifically authorized for such access and email via smartphones or other mobile devices; and
4. Inspect computers, smartphones, and any other media that have been transported outside the United States for compromise prior to any physical or logical connection to any DOJ system. If the component cannot conduct such an inspection, it must reimage the computer or sanitize the media.

E. Classified Information

1. National Security Systems and Sensitive Compartmented Information

Security policy for information systems processing collateral (i.e., non-sensitive compartmented information (SCI)) national security information (NSI) is established by the Committee on National Security Systems (CNSS). Security policy for systems processing SCI is established by the DNI CIO in Intelligence Community Directive (ICD) 503, “Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation.” The FBI CIO will serve as the AO for all DOJ SCI systems. The certification authority and Information System Security Manager (ISSM) function for SCI systems, excluding the FBI systems, reside solely with the DOJ OCIO, CSS.

Components must conform to the DOJ SPOM, ICDs, Intelligence Community Policy Guidance, Intelligence Community Policy Memorandums, and CNSS policies to manage the security of their national security systems. Components must use NIST SP 800-59, “Guideline for Identifying an Information System as a National Security System,” to identify national security systems.

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

The component CIO or, for a component without a CIO, the official at the Executive Officer or equivalent level, must approve, in writing, the processing of classified (collateral) information on standalone laptops, mobile computing devices, and removable media. Standalone laptops, mobile computing devices, and removable media processing SCI must obtain approval from the FBI CIO. Requests for approval must be routed to the DOJ CISO who will obtain the approval from the DOJ CIO or FBI CIO as necessary. “DOJ Information Technology Security Standard – Classified Laptop and Standalone Computers Security Policy” outlines the requirements for laptop computers and standalone computers that process or store classified information. If security requirements outlined in the Classified Laptop and Standalone Computers Security Policy are not met, waivers must be approved by the component CIO with concurrence from the Head of Component or Principal Deputy and DOJ CIO.

3. Facsimile Transmission

- a. All classified and sensitive facsimile transmissions must be preceded by a cover sheet that contains the following information:

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

F. Cloud Computing

Unclassified systems within DOJ that use cloud technologies and connect to the production network or process, store, or transmit DOJ information must adhere to the requirements identified in FISMA, NIST, and Federal Risk and Authorization Management Program (FedRAMP) documentation. DOJ components are required to use cloud service providers (CSPs) that have a provisional ATO from the FedRAMP Joint Authorization Board, an Agency ATO, or a CSP ATO. If the CSP does not have one of these provisional ATOs, the CSP must work with the component to ensure FedRAMP compliance. DOJ and component AOs hold ultimate responsibility to issue the final ATO for each system.

All component FedRAMP information must be entered into the DOJ system of record or other DOJ-approved Information Security Continuous Monitoring tool. In addition, all CSPs must comply with the DOJ's Trusted Internet Connection (TIC) requirements, either through the use of a DOJ-approved TIC or through the DOJ Cloud Security Infrastructure.

Mission Essential Systems and information systems categorized as FIPS 199 High that are in a non-DOJ managed cloud must replicate their data to the DOJ Core Enterprise Facilities (CEFs).

DOJ requires the use of PGD 15-03 (or its latest iteration) in all solicitations, including those for cloud services, unless waived, in whole or in part, by the SPE. PGD 15-03 aligns with the DOJ Cloud Security Instruction and includes specific clauses that require CSPs to comply with FISMA, NIST, and FedRAMP requirements.

G. 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 140-2 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. Information on mobile devices that is categorized as “federal record information” must be managed in accordance with applicable records retention schedules and departmental and component policies on capture and retention of the information.

H. External Information Systems

1. External information systems are information systems or parts of information systems that are outside the authorization boundary established by the component. The component typically has no direct control over the application of required security controls or the assessment of security control effectiveness. External access includes interconnections between DOJ information systems and non-DOJ information systems and between separate internal DOJ information systems where there is direct connection of two or more information systems for the purpose of sharing data and other information resources.
2. External access also includes connections to the Internet.
3. External access presents both security concerns and resource management issues. The goal of this policy is to ensure that components can effectively, efficiently, and safely exchange data with other government and private sector systems and can use resources available on the Internet to accomplish their missions.
4. System and Communications Protection

Connections to external networks that support access to DOJ hosted resources must be obtained through a TICAP or the Cloud Security Infrastructure, unless the DOJ CIO grants a waiver based upon assessed risk, mitigation controls, and operational requirements.

5. Components are:
 - a. Required to obtain all connections to external information systems and networks in accordance with the provisions of DOJ security requirements; and
 - b. Prohibited from deploying systems, technologies, or services that are inconsistent with DOJ security architecture requirements, unless the DOJ CIO

grants a waiver based upon assessed risk, mitigating controls, and operational requirements prior to operational use.

III. Implementing the Risk Management Framework for DOJ Systems

The standard security and privacy control requirements described in this Order are applicable to all DOJ information systems. DOJ information systems that process NSI must meet any additional requirements specified by the CNSS. DOJ information systems that process SCI must meet any additional requirements specified by the DNI. If there is a conflict in requirements for systems processing NSI or SCI, the CNSS or DNI requirements govern. Components must use NIST SP 800-59, “Guideline for Identifying an Information System as a National Security System,” to identify national security systems.

A. Categorize Information Systems

1. Components must categorize all DOJ information systems as low-, moderate-, or high-impact in accordance with FIPS 199 and 200 or applicable standards for national security systems, as implemented in DOJ’s system of record. This process establishes security categories for information types and information systems. The security categories are based on the potential impact on a component if certain events occur that jeopardize the information and information systems needed by the component to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. The categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII will depend on the sensitivity of the PII, the privacy risks, and the associated risk to agency operations, agency assets, other organizations, and the Nation. The impact value for a system must be the highest value (i.e., high water mark) of all values assigned to the types of information resident on the system or as otherwise determined based on the component’s program and requirements.
2. The component’s risk assessment and mission criticality indicators are given consideration regarding any required adjustments in the categorization results. Rationale for deviations from the recommended security categorizations must be documented in the system security and privacy plans (SSPP). Designated senior-level officials within the component, as defined by the DOJ-approved security assessment and authorization process, must review and approve the categorizations. Documented results of this approval must be captured in the SSPP.

B. Select Security and Privacy Controls

1. DOJ has developed cybersecurity and privacy standards based on the security and privacy control families outlined in federal and national standards, supplemented with additional DOJ standards. The *DOJ Cybersecurity Standards* outline, in specific detail, the requirements for achieving the high-level goals within this Order. These standards represent minimum DOJ information system security and privacy control requirements, supplement this Order, and are required to be used in accordance with the terms and conditions therein. The requirements in the standards are implemented in DOJ's system of record.
2. Subsequent to the categorization process, components must select an appropriate set of security and privacy controls and assurance requirements for their information systems that: (1) satisfy the minimum security and privacy requirements set forth in these standards, and (2) are tailored (enhanced or limited) based on the results of a risk assessment and local conditions, including component- or system-specific security and privacy requirements, specific threat information, cost-benefit analyses, and any special circumstances.
3. The AO for the information system must determine if the control-set identified in the information system security plan is appropriate for securing the information system to an acceptable level of operational risk to the component. The CPCLLO, or a duly authorized official, must review and approve the privacy plans for information systems prior to authorization, reauthorization, or ongoing authorization. Components must document the AO's and CPCLLO's approval of the initial set of tailored security and privacy controls in the SSPP, including the component's rationales for any refinements or adjustments to the baseline set of controls.

C. Implement Security and Privacy Controls

Components must then implement the security and privacy controls in the information system in accordance with the SSPP. AOs are better positioned to make mission risk determinations based on the known vulnerabilities remaining in the information system after the agreed-upon set of security controls is implemented. Also, the CPCLLO, or a duly authorized official, is better positioned to make mission risk determinations based on the known vulnerabilities remaining in the information system after the agreed-upon set of privacy controls is implemented.

D. Assess Security and Privacy Controls

Components must assess the security and privacy controls using appropriate methods and procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and organization. Components must document assessments of all selected and implemented controls prior to the operation of the information system, and periodically thereafter, consistent with the frequency defined in the agency continuous monitoring strategy and the agency risk tolerance.

E. Authorize Information System

The system AO must make an authorization decision whether or not to accept the risk for the information system operation based on the potential impact of the risk to departmental operations and assets, individuals, other organizations, and the Nation. The CPCLCLO, or a duly authorized official, must review 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 the AO makes a risk determination and acceptance decision.

F. Monitor Security and Privacy Controls

1. Components must monitor the information system on a continuous basis for changes to the information system or its operational environment, the information system security and privacy plan boundaries, or other conditions (e.g., threat and risk factors). Components must conduct security impact analyses of the associated changes, update the information system security plan (and other relevant information system documentation, such as the system privacy plan, as appropriate), and report changes in the security or privacy status of the system to appropriate officials on a regular basis.
2. Significant changes to the system require reauthorizations by the component AO. Significant changes that effect an information system's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of PII must be reviewed and assessed by the CPCLCLO, or a duly authorized official, prior to reauthorization by the AO. Examples of changes to an information system that should be reviewed for possible reauthorization include:
 - a. Installing a new or upgraded operating system, middleware component, or application;

- b. Modifying system ports, protocols, or services;
 - c. Installing a new or upgraded hardware platform or firmware component;
 - d. Modifying cryptographic modules or services;
 - e. Adding connections to information systems outside the accreditation boundary; and
 - f. Making functional changes or enhancements to the system that affect its mission criticality, information types, user base, or classification of data supported by the information system.
3. Changes in laws, directives, policies, or regulations, while not always directly related to the information system, can also potentially affect the security of the system and trigger a reauthorization action.
 4. Reauthorization should be avoided in situations where the continuous monitoring process provides the necessary and sufficient information to AOs to manage the potential risk arising from the information system changes.
 5. Components must appropriately plan and budget to upgrade, replace, or retire information systems if the protections for the system cannot be effectively implemented commensurate with the potential risks arising from the system. Components must ensure that the appropriate officials are made aware, in a timely manner, of information and information systems that cannot be appropriately protected or secured, and that such systems are given a high priority for upgrade, replacement, or retirement.

IV. Roles and Responsibilities

A. DOJ Chief Information Officer

The DOJ CIO serves as the Deputy Assistant Attorney General, Information Resources Management (DAAG/IRM). In this role, the DOJ CIO advises and assists the Attorney General (AG), the Deputy AG (DAG), the Assistant AG 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 all applicable federal laws and directives. These functions are inherently governmental and therefore must be assigned to government personnel only. In addition to the responsibilities outlined in DOJ Order 0903, Information Technology Management, the DOJ CIO's include:

1. Developing, implementing, and managing a DOJ-wide POA&M process to correct cybersecurity weaknesses;
2. 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 destruction of:
(a) information collected or maintained by or on behalf of DOJ, and (b) IT systems used or operated by an agency, a contractor of an agency, or another organization on behalf of an agency;
3. Enforcing departmental cybersecurity policy, including levying sanctions on components for non-compliance;
4. Developing and maintaining a central repository of information on new and emerging technologies;
5. Coordinating the evaluations of new and emerging technologies by components;
6. 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 annual cybersecurity awareness training;
7. Ensuring cybersecurity management processes are integrated with DOJ and/or component strategic and operational planning processes;
8. 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 IT systems;
9. 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 IT systems);
10. Approving encryption technologies that are not FIPS 140-2 validated in those situations where FIPS-validated products are not available;
11. Appointing a CISO to carry out the DOJ-wide IT security program, as required by FISMA;
12. Taking appropriate action if a component, contractor, or other non-DOJ organization or its representative is found to be non-compliant with DOJ cybersecurity policy;

13. Establishing a Cybersecurity Committee with supporting project teams composed of lead-component cybersecurity personnel, such as component CIOs; and
14. Reporting to the AG and OMB on the status of the DOJ's Cybersecurity Program.

The DOJ CIO may delegate any cybersecurity-related responsibilities listed above to the DOJ CISO.

B. DOJ Chief Information Security Officer

The DOJ CISO is responsible for the management and oversight of the DOJ cybersecurity program and its associated activities, including those delegated by the DOJ CIO. The CISO chairs the DOJ's Cybersecurity Committee, which is chartered under the DOJ CIO Council, and the Continuous Monitoring Working Group. Additionally, the CISO serves as the principal lead for DOJ to implement FISMA requirements. These functions are inherently governmental and therefore must be assigned to government personnel only. The CISO also serves as the DOJ CIO's liaison to federal agencies for all matters related to the implementation of 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 policy and procedures for related controls to cost-effectively reduce risks to an acceptable level;
3. Monitoring, evaluating, and periodically testing information system security 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 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 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 at least quarterly, in accordance with guidance issued by the DOJ CIO, on the status of the information systems compliance with the Cybersecurity Program to the DOJ CIO.

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 be assigned to government personnel only. 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. Providing advice and recommendations to the DOJ CIO on waiver requests;
3. 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
4. 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, IT Management.

D. Head of Component or Designee(s)

The Head of Component, or his or her designee(s), must establish and maintain a component-wide cybersecurity program to secure the component's IT 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 his or her 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 Management Plan at the component and system levels and reporting results in accordance with OCIO guidelines;
3. Ensuring that monitoring, testing, and evaluating the effectiveness of cybersecurity policy, procedures, practices, and security controls, which are to be performed with a frequency depending on risk, are completed as directed by CSS;
4. Ensuring the completion of periodic assessments of risk, including the magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information and IT systems that support DOJ's operations and assets;
5. Developing, implementing, managing, and prioritizing corrective POA&Ms to correct known weaknesses in cybersecurity using the DOJ-wide POA&M process;
6. Reporting quarterly to the DOJ CIO and CISO, in accordance with guidance issued by the Justice Management Division or the DOJ CIO, on the status of their Cybersecurity Programs;
7. Integrating security in the Capital Planning and Investment Control process;
8. Ensuring that roles and responsibilities within the component are assigned (e.g., component Cybersecurity Committee member, component CIO, AO, Certification Agent, information system owner, information owner, user representative, and Information System Security Officer);
9. Coordinating with the DOJ OCIO on any evaluations of new technologies that could impact DOJ or enterprise services;

10. 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;
11. Establishing procedures to ensure that software installed on component IT systems is in compliance with applicable copyright laws and is incorporated into the IT system's life cycle management process;
12. 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 IT systems and monitoring these waivers
13. 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 annual cybersecurity awareness training.

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 DOJ's privacy policy and standards, consistent with applicable law, regulation, and administration policy and in consideration of the Fair Information Practice Principles (FIPPs). The CPCLO is the principal advisor to DOJ leadership and components on privacy and civil liberties matters affecting DOJ's mission and operations and fulfills the statutory duties set forth in the previously stated regulation.

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 latest iteration), 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 to 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 Publication 199 and SP 800-60, the categorization of information systems that create, 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 prior to 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 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 an agency across the agency risk management tiers to ensure continued compliance with applicable privacy requirements; and (b) 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 any designated component official, including the OPCL Director, the Heads of Components, the DOJ CIO, the DOJ CISO, or the Senior Component Officials for Privacy (SCOP), so long as such delegation is consistent with federal law and DOJ policy and subject to the CPCLO's oversight and control.

APPENDIX: AUTHORITIES

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

Presidential and Office of Management and Budget Circulars
OMB Circular A-11: Preparation of Federal Budgets, Strategic Plans, Annual Performance Plans/Annual Program Performance Reports, July 2011.
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.

Presidential and Office of Management and Budget Memoranda
M-03-18: Implementation Guidance for the E-Government Act, August 2003.
M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003).
M-03-22: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 2003.
M-04-04: E-Authentication Guidance, December 2003.
M-04-16: Software Acquisition, July, 2004.
M-04-19: IT Project Manager Qualification Guidance, July 2004.
M-04-26: Personal Use Policies and File Sharing Technology, September 2004.
M-05-08, Designation of Senior Agency Officials for Privacy (Feb. 11, 2005);
M-05-22: Transition Planning for Internet Protocol v6, August 2005.
M-05-23: Improving Information Technology Project Planning and Execution, August 2005.

Presidential and Office of Management and Budget Memoranda

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-06-16: Protection of Sensitive Agency Information, June 2006.

M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007);

M-08-01: HSPD-12 Implementation Status, October 2007.

M-08-26: Transition from FTS-2001 to Networx, August 2008.

M-08-27: Guidance for Trusted Internet Connection (TIC) Compliance, September 2008.

M-09-02: Information Technology Management Structure and Governance Framework, October 2008.

M-09-32: Update on Trusted Internet Connections Initiative, September 2009.

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.

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-11-11: Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors, February 2011.

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

M-12-10: Implementing PortfolioStat, March 31, 2012.

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

M-14-03, Enhancing the Security of Federal Information and Information Systems, November 18, 2013

M-15-01, Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices, October 3, 2014

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

DOJ Orders, Policy Statements and Instructions

DOJ Order 2830.4, Administrative Computer Support for Handicapped Employees, March 4, 1987.

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

DOJ Order 2740.1A, Use and Monitoring of DOJ Computers, November 30, 2010.

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

DOJ Policy Statement 900.01, Data Center Facilities Enhancement and Relocation of Information Technology Infrastructure, November 14, 2013.

DOJ Order 0601, Privacy and Civil Liberties, February 6, 2014.

DOJ Order 0801.04, Electronic Mail Records Retention, May 8, 2015.

DOJ Order 0903 Information Technology Management, May 5, 2016.

Federal/Departmental Regulations/Guidance

Department of Homeland Security Trusted Internet Connections (TIC) Reference Architecture v2.0, October 1, 2013.

Department of Justice Strong Authentication Plan, May 2016.

DOJ Mobile Device and Mobile Application Security Instruction, July 2015.

NIST FIPS SP 199: Standards for Security Categorization of Federal Information and Information Systems.

NIST SP 800-12: An Introduction to Computer Security: The NIST Handbook.

NIST SP 800-30 Revision 1: Guide for Conducting Risk Assessments.

NIST SP 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems.

NIST SP 800-39: Managing Information Security Risk: Organization, Mission, and Information System View.

NIST SP 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems.

NIST SP 800-53A Revision 4: 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.

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

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