INFORMATION DIRECTIVE
PROCEDURE

Information Security – Program Management Procedures		
Directive No.: 2150-P-23.0	CIO Approval: 12/19/2016	Transmittal No.: 17-002

Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated 07/07/2005

Information Security – Program Management Procedures

1. PURPOSE

To extend and provide specificity to the Environmental Protection Agency (EPA) Information Security Policy. This document shall be used to develop procedures, standards and guidance that facilitate the implementation of security control requirements for the Program Management (PM) control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

2. SCOPE

These procedures cover all EPA information and information systems to include information and information systems used, managed, or operated by a contractor, another agency, or another organization on behalf of the agency.

These procedures apply to all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of the EPA.

3. AUDIENCE

The audience is all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of the EPA.

4. BACKGROUND

Based on federal requirements and mandates, the EPA is responsible for ensuring that all offices within the Agency meet the minimum security requirements defined in the *Federal Information Processing Standards* (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. All EPA information systems shall meet security requirements through the use of the security controls defined in the NIST SP 800-53, Revision 4. This document addresses the procedures and standards set forth by the EPA, and complies with the Program Management family of controls.

5. AUTHORITY

The information directive is issued by the EPA Chief Information Officer (CIO), Pursuant to Delegation 1-19, dated 07/07/2005.

Additional legal foundations for the procedure include:

- E-Government Act of 2002, Public Law 107-347, Title III, Federal Information Security Management Act, as amended
- Federal Information Security Modernization Act of 2014, Public Law 113-283, chapter 35 of title 44, United States Code (U.S.C.)
- Freedom of Information Act (FOIA), 5 U.S.C. § 552, as amended by Public Law 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996
- Clinger-Cohen Act of 1996, Public Law 104-106
- Paperwork Reduction Act of 1995 (44 U.S.C. 3501-3519)
- Privacy Act of 1974 (5 U.S.C. § 552a) as amended
- USA PATRIOT Act of 2001, Public Law 107-56
- Code of Federal Regulations, Part 5 Administrative Personnel, Subpart C—Employees Responsible for the Management or Use of Federal Computer Systems, Section 930.301 through 930.305 (5 C.F.R. 930.301-305)
- Office of Management and Budget (OMB) Memorandum M-02-01, “Guidance for Preparing and Submitting Security Plans of Action and Milestones”, October 2001
- OMB Memorandum M-06-19, “Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments”, July 2006
- OMB Memorandum M-07-16, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information”, May 2007
- OMB Memorandum M-10-28, “Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS)”, July 2010
- OMB Memorandum M-15-14, “Management and Oversight of Federal Information Technology”, June 2015
- OMB Circular A-130, “Management of Federal Information Resources,” Appendix III, “Security of Federal Automated Information Resources”, November 2000
- Homeland Security Presidential Directive (HSPD)-7, Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003
- HSPD-23, Cyber Security and Monitoring, January 8, 2008
- Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- EPA Information Security Program Plan
- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures
- EPA Information Security Continuous Monitoring Strategic Plan
- CIO Policy Framework and Numbering System

6. PROCEDURE

The "PM" designator identified in each procedure represents the NIST-specified identifier for the Program Management control family, as identified in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.*

PM-1 – Information Security Program Plan

1) The Senior Agency Information Security Officer (SAISO), under direction of the CIO and in coordination with the EPA Administrator, Assistant Administrators (AA), Regional Administrators (RA), Director of Office of Information Technology Operations (OITO), Information Owners (IO), Information Security Officers (ISO), System Owners (SO) and Information System Security Officers (ISSO), for EPA-operated systems, shall:

    a) Develop and disseminate an organization-wide information security program plan that:

        i) Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;

        ii) Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;

        iii) Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and

        iv) Is approved by a senior official who is responsible and accountable for the risk being incurred to EPA operations (including mission, functions, image, and reputation), EPA assets, individuals, other organizations, and the Nation.

    b) Review the organization-wide information security program plan at least annually.

    c) Update the plan to address organizational changes and problems identified during plan implementation or security control assessments.

    d) Protect the information security program plan from unauthorized disclosure and modification.

PM-2 – Senior Information Security Officer

1) The Agency CIO, in coordination with the Chief Financial Officer (CFO) shall:

    a) Appoint a SAISO with the mission and resources to coordinate, develop, implement and maintain an organization-wide information security program.

PM-3 – Information Security Resources

1) The SAISO, in coordination with the CIO, CFO, Senior Budget Officers (SBO), Information Management Officer (IMO), Director of OITO, Senior Information Official (SIO), SOs, IOs, ISOs, and ISSOs, for EPA-operated systems, shall; and Service

Managers (SM), in coordination with IOs for systems operated on behalf of the EPA,[1] shall ensure service providers:

a) Determine the resources needed to implement the organization's information security program and include the resource request in capital planning and investment control processes and documents.

i) Employ a business case to justify and record the resources required.

ii) Ensure information security resources are available for expenditure, as forecasted and planned, and plan for contingencies in the event that resources are not available.

b) The requirement applies to all EPA Program Offices and Regions.

PM-4 – Plan of Action and Milestones Process

1) The SAISO, in coordination with ISOs, shall:

a) Implement an enterprise process for ensuring that plans of action and milestones for the security program and information systems transmitting, processing or storing agency information:

i) Are developed and maintained;

ii) Document the remedial information security actions to adequately respond to risks to agency operations and assets, individuals, other organizations, and the Nation; and

iii) Are reported in accordance with OMB Federal Information Security Modernization Act (FISMA) reporting requirements.

b) Review plans of action and milestones for consistency with the agency's risk management strategy and agency-wide priorities for risk response actions, and take actions accordingly where inconsistencies exist.

c) Employ the enterprise process for ensuring that Plans of Action and Milestones (POA&M) for each Program Office or Region (PO/R) information systems are developed and maintained.

d) Ensure SOs, IOs, and SMs:

i) Implement remedial information security actions, and

ii) Report POA&Ms in accordance with FISMA reporting requirements.

e) Review their respective PO/R information systems' POA&Ms for consistency with the agency risk management strategy, agency priorities for risk response, and risk response actions and eliminate inconsistencies.

f) Notify the ISO and system Point of Contact (POC) if POA&Ms are reopened.

PM-5 – Information System Inventory

1) The SAISO, in coordination with ISOs and SMs, shall:

a) Develop and maintain an inventory of agency information systems in accordance with FISMA reporting requirements.

[1] *Information Owners and Service Managers shall follow FedRAMP requirements for all services obtained where EPA information is transmitted, stored or processed on non-EPA operated systems.*

PM-6 – Information Security Measures of Performance

1) The SAISO shall:
   a) Develop, monitor and report on the results of information security measures of performance in accordance with NIST SP 800-55, *Security Metrics Guide for Information Technology Systems*, and NIST SP 800-80, *Guide to Developing Performance Metrics for Information Security*.

PM-7 – Enterprise Architecture

1) The SAISO, in coordination with the EPA Chief Architect, shall:
   a) Develop an Information Security Enterprise Architecture with consideration for current information security threats and risks to organizational operations, assets, information and individuals.

PM-8 – Critical Infrastructure Plan

1) The SAISO, in coordination with the CIO, SIOs, SOs, IOs, SMs, ISOs and ISSOs, shall:
   a) Identify agency assets and resources that meet the definition of critical infrastructure.
   b) Develop, document, and update the agency critical infrastructure plan to protect key infrastructure resources.

PM-9 – Risk Management Strategy

1) The SAISO, in coordination with the EPA Deputy Administrator and the CIO, shall:
   a) Develop a comprehensive strategy to manage risk to Agency operations and assets, individuals, other organizations, and the Nation, associated with the operation and use of information systems.
   b) Implement a risk management strategy across the Agency.
   c) Review and update the risk management strategy at least annually or more frequently to address significant organizational changes.

PM-10 – Security Authorization Process

1) The SAISO, in coordination with SIOs, Common Control Providers (CCP), SOs, SMs, IOs, ISOs and ISSOs, shall:
   a) Manage (i.e., document, track, and report) the security state of organizational information systems and the environments in which those systems operate through the Agency’s security authorization processes.
   b) Designate individuals to fulfill specific roles and responsibilities within the organizational security authorization process.
   c) Integrate the security authorization processes into an organization-wide risk management program.

PM-11 – Mission/Business Process Definition

1) The SAISO, in coordination with the SIOs, IOs, ISOs, IMOs and Information Resource Management Branch Chiefs (IRMBC), shall:
    - a) Define mission/business processes with consideration for information security and the resulting risk to agency operations, assets, individuals, other organizations and the Nation.
    - b) Determine information protection needs arising from the defined mission/business processes, and revise the processes as necessary until achievable protection needs are obtained.

PM-12 – Insider Threat Program

1) The SAISO, in coordination with OA, OARM, OCFO, SIOs, and ISOs, shall:
    - a) Implement an insider threat program that includes a cross-discipline insider threat mitigation and response team.

PM-13 – Information Security Workforce

1) The SAISO, in coordination with OARM, SIOs, and ISOs, shall:
    - a) Establish an information security workforce development program.
    - b) Define the knowledge and skill level requirements to perform information security duties and tasks.
    - c) Assign information security roles and responsibilities to appropriately trained and experienced personnel.
    - d) Develop an organizational role-based training program for individuals assigned information security roles and responsibilities.
    - e) Provide standards for measuring and building individual qualifications for organizational information security-related positions.
    - f) Ensure organizational information security workforce personnel obtain and continue to meet individual qualification standards for their assigned organization information security roles.
    - g) Ensure information security workforce personnel obtain and maintain certification and training on an ongoing basis.
    - h) Annually reevaluate the organization's workforce's knowledge and skill requirements based upon current risks and threats, and organization environment changes.
    - i) Ensure that data and information system owners are notified of changes affecting the information security workforce.
    - j) Prioritize requirements for the development of training content to address the organization's information security workforce gaps and deficiencies.

PM-14 – Testing, Training, and Monitoring

1) The SAISO, in coordination with the OARM SIOs, and ISOs, shall:
    - a) Develop, implement and maintain plans for conducting security testing, training, and monitoring activities associated with agency information systems.

b) Ensure plans are executed in a timely manner.

c) Review testing, training and monitoring plans for consistency with the agency risk management strategy and agency-wide priorities for risk response actions.

PM-15 – Contacts with Security Groups and Associations

1) The SAISO, in coordination with OARM, SIOs and ISOs, shall:

   a) Facilitate ongoing security education and training for all agency personnel.

   b) Maintain understanding of current recommended security practices, techniques and technologies.

   c) Gather and disseminate current security-related information including threats, vulnerabilities and incidents.

PM-16 – Threat Awareness Program

1) The SAISO, in coordination with OARM and ISOs, shall:

   a) Implement a threat awareness program that includes a cross-agency information-sharing capability.

7. ROLES AND RESPONSIBILITIES

Chief Architect

1) The Chief Architect has the following responsibilities with respect to program management:

   a) Coordinate with the SAISO to develop and implement the Agency's information security architecture.

   b) Facilitate the integration of information security into all layers of enterprise architecture to ensure the Agency implements secure solutions.

Chief Financial Officer (CFO)

1) The CFO has the following responsibilities with respect to program management:

   a) Assist the CIO in appointing a SAISO with the mission and resources to coordinate, develop, implement and maintain an organization-wide information security program.

Chief Information Officer (CIO)

1) The CIO has the following responsibilities with respect to program management:

   a) Appoint a SAISO responsible for EPA information security program management.

   b) Ensure the EPA information security program and protection measures are compliant with FISMA and related information security directives.

   c) Develop, document, implement, and maintain an Agency-wide information security program as required by EPA policy, FISMA, and related information security directives, to enable and ensure EPA meets information security requirements.

   d) Develop, document, implement, and maintain Agency-wide, well-designed, well-managed continuous monitoring and standardized risk assessment processes.

e) Develop, maintain, and issue Agency-wide information security policies, procedures, and control techniques to provide direction for implementing the requirements of the information security program.

f) Assist senior Agency and other key officials with understanding and implementing their information security responsibilities.

g) Establish minimum mandatory risk-based technical, operational, and management information security control requirements for Agency information and information systems.

h) Coordinate resource allocation efforts with OCFO as required.

i) Designate a SAISO whose primary duty is information security.

j) Ensure that the SAISO possesses and maintains professional qualifications, including training and experience, required to administer the EPA Information Security Program functions and carry out the CIO responsibilities under EPA policy and relevant information security laws, Executive Branch policy and other directives.

k) Report annually, in coordination with the AAs, RAs and other key officials, to the EPA Administrator on the effectiveness of the EPA Information Security Program, including progress of remedial actions.

l) Serve as the Risk Executive for the Agency's information security Risk Executive Function. As such, coordinate with the Risk Executive Group, SAISO, SIOs, IMOs, ISOs, and SOs to govern risk.

Common Control Providers (CCP)

1) CCPs have the following responsibilities with respect to program management:

a) Document common controls in security plans.

b) Coordinate with the CIO, SAISO, information owners and service managers regarding information security requirements. Determine and carry out responsibilities for defining, developing, documenting, implementing, assessing and monitoring all controls to include common and hybrid controls.

c) Develop, implement, assess, configure, monitor and maintain the organization's security control requirements in accordance with the information system's security categorization level (i.e., Low, Moderate or High).

d) Coordinate with information owners to ensure systems are properly categorized according to information categorizations.

e) Coordinate with information owners to identify controls required to protect information stored, processed, or transmitted by assigned systems adequately.

f) Deploy and operate systems according to the security requirements documented in security plans.

g) Assess all controls prior to systems becoming operational and a subset of all controls, including core controls, annually thereafter, at a minimum. Ensure control assessments are conducted by third party control assessors for moderate and high-categorized systems. Obtain security assessment reports from assessors.

h) Develop and manage plans of actions and milestones for discovered weaknesses.

i) Coordinate with the Director of OITO to develop, document, and maintain mandatory configurations for information technology (IT) products and solutions used by EPA.

j) Coordinate with the Director of OITO to establish, manage, and use enterprise configuration change management capabilities for all IT used by EPA.
k) Coordinate with the SAISO in responding to information security data calls, audit requests, and reporting.
l) Coordinate with the CIO, Risk Executive, Risk Executive Group, SAISO and others involved with securing Agency information and systems to ensure risks are managed to an acceptable level.
m) Provide security plans, security assessment reports, and plans of action and milestones to information owners and system owners inheriting common controls.

Senior Agency Information Security Officer (SAISO)

1) The SAISO has the following responsibilities with respect to program management:
   a) Develop, document, implement and maintain an Agency-wide information security program to protect EPA information and information systems.
   b) Develop, document, implement and maintain Agency-wide, well-designed, well-managed continuous monitoring and standardized risk assessment processes.
   c) Ensure enforcement and compliance of information security programs and information systems throughout the Agency with FISMA and related information security laws, regulations, directives, policies, and guidelines.
   d) Develop, maintain, and distribute Agency-wide information security policies, procedures, and control techniques to provide direction for implementing the requirements of the information security program.
   e) Assist senior Agency and other key officials with understanding and implementing information security responsibilities that fall within their realm of oversight.
   f) Establish minimum, mandatory risk-based technical, operational, and management information security control requirements for the Agency information security program, information, and information systems.
   g) Report compliance failures and policy violations directly to the appropriate organizational officials for appropriate disciplinary and corrective actions.
   h) Report the effectiveness of the information security program and the progress of remedial actions to the EPA Administrator annually.
   i) Develop, implement, and maintain security authorization and reporting capabilities, including the Agency security information repository, as required by the information security program and applicable policy and procedures.
   j) Develop and maintain role-based training, education and credentialing requirements to ensure personnel with significant information security responsibilities receive adequate training with respect to such responsibilities.
   k) Coordinate with the Director of OITO to ensure the Agency can adequately detect, respond to, and report information security incidents.
   l) Coordinate with independent auditors, audit coordinators, SIOs, IMOs, ISOs, and other key officials to manage audits and audit responses.
   m) Provide guidance to EPA ISOs. Lead periodic meetings to disseminate information, discuss and resolve issues and develop solutions and courses of action for implementing the EPA Information Security Program objectives.
   n) Provide relevant and up-to-date security information periodically to personnel with significant information security responsibilities via standard, internal communication mechanisms.

o) Coordinate with the EPA Office of Inspector General to ensure the EPA information security program and protection measures are compliant with FISMA and related information security directives.

p) Coordinate with the EPA Privacy Officer during security incidents involving Personally Identifiable Information (PII) and to identify EPA Information Security Program related controls and processes that support EPA's Privacy Program objectives.

q) Coordinate with EPA leadership and officials as needed to implement and improve information security program effectiveness.

EPA Administrator, Assistant Administrators, Regional Administrators

1) The EPA Administrator, Assistant Administrators and Regional Administrators have the following responsibilities with respect to program management:

a) Ensure that an Agency-wide information security program is developed, documented, implemented and maintained to protect information and information systems.

b) Provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the Agency and on information systems used, managed or operated by the Agency, another Agency or by a contractor or other organization on behalf of the Agency.

c) Ensure information security management processes are integrated with Agency strategic and operational planning processes.

d) Provide resources to improve information security for the information and information systems that support the operations and assets under their control.

e) Ensure compliance with FISMA and related information security directives.

f) Ensure EPA has trained personnel sufficient to comply with FISMA and other related information security directives.

g) Ensure annual Inspector General FISMA information security audit results are reported to Congress, OMB, DHS, and other entities as required by law and Executive Branch direction.

h) Comply with FISMA and other related information security laws and requirements in accordance with the CIO directives. Such CIO directives shall take priority over all routine operational tasks and assignments, and shall be complied with immediately.

i) Ensure all EPA information and information system users within their organizations take immediate action to comply with directives from the CIO to (a) mitigate the impact of any potential security risk, (b) respond to a security incident, or (c) implement the provisions of a Computer Security Incident Response Capability (CSIRC) notification.

Director of Office of Information Technology Operations (OITO)

1) The Director of OITO has the following responsibilities with respect to program management:

a) Develop, maintain, and issue Agency-wide information security procedures and control techniques for Agency-wide and local program office and regional systems and operations to implement and support the Agency information security program and implement SAISO issued policies, procedures and control techniques.

b) Implement, operate and maintain enterprise tools and controls required to support the Agency information security program policies, procedures and control techniques.

c) Define and implement processes to use and maintain enterprise tools and controls.

d) Coordinate with program offices, regions, and other entities as necessary to implement, operate, and maintain enterprise tools, controls, and processes.

e) Ensure the Chief Architect supports developing, maintaining, and implementing the Agency's Information Security Architecture.

f) Monitor for and notify the CIO, SAISO, SIO's and other personnel as appropriate of potential and actual threats to the Agency's information system resources.

g) Ensure that only those information systems having approved authorizations to operate or test are attached to the EPA network.

h) Provide security awareness and role-based training delivery mechanisms and related support.

i) Coordinate with program offices, regions and other entities as appropriate when they implement local controls to ensure compatibility and interoperability with enterprise tools, controls and processes.

j) Lead the development, documentation and maintenance of mandatory configurations for IT products and solutions used by EPA.

Information Owners (IO)

1) IOs have the following responsibilities with respect to program management:

a) Implement policies, procedures and control techniques identified in the Agency information security program.

b) Coordinate with SOs, CCPs and SMs to provide information as needed for developing, maintaining and providing information security documents required under the EPA Information Security Program.

c) Coordinate with SOs, CCPs, SMs and service providers to identify controls required to protect information stored, processed or transmitted by supporting systems. Identify and provide information to SOs, CCPs, SMs and service providers if risk analysis requires additional or more stringent controls than those identified in the set of baseline controls.

d) Ensure service providers' systems supporting non-enterprise services are configured, continuously monitored and maintained to protect supported information within acceptable risks.

e) Follow Federal Risk and Authorization Management Program (FedRAMP) requirements, where applicable.

f) Maintain accurate and up-to-date system security information, such as plans of actions and milestones, system security plans and security assessment reports in the Agency information security information repository for non-enterprise services obtained.

g) Ensure service providers deploy and operate systems according to the security requirements documented in security plans.

h) Ensure all controls are assessed for systems supporting non-enterprise services obtained prior to using service and that a subset of all controls, including core controls, are assessed annually thereafter, at a minimum. Ensure control assessments are conducted by third party control assessors for moderate and high-categorized information and obtain security assessment reports from assessors.

i) Develop and manage and ensure service providers develop and manage plans of actions and milestones for discovered weaknesses for non-enterprise services obtained.

j) Ensure service providers implement mandatory configurations for information technology products and solutions used by EPA for non-enterprise services.

k) Ensure service providers establish, manage and use configuration change management processes for non-enterprise services obtained.

l) Coordinate with the SAISO in responding to information security data calls, audit requests and reporting.

m) Coordinate with the CIO, SAISO, CCPs, SOs, SMs and service providers regarding information security requirements and determine and carry out responsibilities for defining, developing, documenting, implementing, assessing and monitoring all controls to include common and hybrid controls.

Information Systems Security Officers (ISSO)

1) ISSOs have the following responsibilities with respect to program management:

a) Develop and maintain in coordination with system administrators and others involved with implementing and maintaining controls, the system security plan, including appendices, the contingency plan and other documents required for information systems' authorization packages.

b) Ensure systems have an authorization to operate or authorization to test from the appropriate SIO prior to use or testing in an operational environment.

c) Enter into the Agency information security information repository all system security information such as plans of actions and milestones, system security plans and security assessment reports and maintain current and accurate information.

d) Coordinate with the CIO, Risk Executive, Risk Executive Group, SAISO and others involved with securing Agency information and systems to ensure risks are managed to an acceptable level.

e) Respond to information security data calls, audit requests, and reporting.

f) Serve as a principal advisor on all matters involving the security of information, information system, or services assigned.

g) Implement policies, procedures and control techniques identified in the Agency information security program.

Information Security Officers (ISO)

1) ISOs have the following responsibilities with respect to program management:
   a) Coordinate with the SAISO in developing, documenting, implementing and maintaining an office, region or Agency-wide information security program to protect EPA information and information systems.
   b) Coordinate with the SAISO in responding to information security data calls, audit requests and reporting.
   c) Implement policies, procedures and control techniques identified in the Agency information security program.
   d) Provide guidance on the roles, responsibilities and Agency information security program requirements for ISSOs, system administrators and others with significant security responsibilities.
   e) Track and ensure all EPA information system users within their organizations successfully complete information security awareness training prior to initial access to EPA systems and information and at least annually thereafter to maintain access. Ensure access is removed for users who do not successfully complete awareness training.
   f) Track and ensure all employees within their organizations designated as having significant information security responsibilities complete role-based information security training and credentialing as defined under the EPA Information Security Program.
   g) Review the Agency information security system inventory tool periodically and ensure systems are reported accurately and completely.
   h) Periodically review the Agency information security information repository and ensure all system security information, such as plans of actions and milestones, system security plans and security assessment reports are entered and maintained accurately and kept up to date.
   i) Coordinate with the CIO, Risk Executive, Risk Executive Group, SAISO and others involved with securing Agency information and systems to ensure risks are managed to an acceptable level.
   j) Monitor POA&Ms to ensure weakness remediation and mitigations are managed and actions are documented properly.
   k) Provide expert advice in developing and updating enterprise and local information security documents to include policy, procedures, standards and guidance.
   l) Support SOs, IOs, and SMs in developing and maintaining system information security documentation, obtaining and maintaining authorization to operate or test and ensuring systems are configured, continuously monitored and maintained to protect supported information within acceptable risks.

Service Managers (SM)

1) SMs have the following responsibilities with respect to program management:
   a) Implement policies, procedures and control techniques identified in the Agency information security program.

b) Ensure procedures, control techniques and other countermeasures as necessary to support and implement Agency information security program requirements are developed and implemented for enterprise services.

c) Coordinate with information owners to decide who has access to the service (and with what types of privileges or access rights) and ensure service users and support personnel receive the requisite security training (e.g., instruction in rules of behavior).

d) Coordinate with information owners to determine if additional rules of behavior are needed beyond those provided in the national rules of behavior and service providers' rules of behavior for particular services. If additional rules of behavior are needed SMs shall coordinate with information owners to establish and publish the additional rules of behavior.

e) Coordinate with the CIO, CCPs, information owners, system owners, other SMs, and service providers regarding information security requirements. Determine and carry out responsibilities for defining, developing, documenting, implementing, assessing and monitoring common and hybrid controls.

f) Ensure service providers' systems supporting enterprise services are configured, continuously monitored and maintained to protect information stored, processed or transmitted within acceptable risks adequately.

g) Coordinate with IOs to ensure service providers' systems supporting non-enterprise services are configured, monitored and maintained to protect supported information stored, processed or transmitted within acceptable risks adequately.

h) Ensure terms of service and other contractual agreements satisfy the security and privacy requirements applicable to EPA systems and information.

i) Follow FedRAMP requirements where appropriate.

j) Coordinate with information owners to ensure systems are properly categorized according to information categorizations for enterprise services.

k) Coordinate with information owners to identify controls required to protect information stored, processed or transmitted by service providers' systems for enterprise services.

l) Ensure service providers deploy and operate systems according to the security requirements documented in security plans.

m) Develop and manage and ensure service providers develop and manage plans of actions and milestones for discovered weaknesses for enterprise services.

n) Conduct or ensure service providers conduct impact analyses for proposed or actual changes to systems or their operational environments for enterprise services.

o) Ensure service providers implement mandatory configurations for IT products and services used by EPA for enterprise services.

p) Ensure service providers establish, manage and use configuration change management processes for enterprise services.

q) Coordinate with the Director of OITO for implementing, operating and maintaining enterprise tools and controls for enterprise services.

r) Coordinate with the CIO, SAISO and others involved with securing Agency information and systems to ensure risks are managed to an acceptable level.

Senior Budget Officers (SBO)

1) SBOs have the following responsibilities with respect to program management:

   a) Assist in determining the resources needed to implement the organization's information security program and include the resource request in capital planning and investment control processes and documents.

Senior Information Officers (SIO)

1) SIOs have the following responsibilities with respect to program management:

   a) Assist in determining the resources needed to implement the organization's information security program and include the resource request in capital planning and investment control processes and documents.

   b) Assist in identifying agency assets and resources that meet the definition of critical infrastructure.

System Owners (SO)

1) SOs have the following responsibilities with respect to program management:

   a) In coordination with the SAISO determine the resources needed to implement the organization's information security program and include in capital planning and investment control processes and documents.

   b) Implement remedial information security actions.

   c) Report POA&Ms in accordance with OMB FISMA reporting requirements.

   d) In coordination with the SAISO identify agency assets and resources that meet the definition of critical infrastructure and develop, document and update an agency critical infrastructure plan to protect key infrastructure resources.

   e) In coordination with the SAISO and ISO manage the security state of organizational information systems and the environments in which those systems operate through the Agency's security authorization processes.

8. RELEVANT DOCUMENTS

- NIST Special Publications, 800 Series
- The National Strategy to Secure Cyberspace, February 2003 - https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

9. DEFINITIONS

- **Information Security:** the practice of defending information from unauthorized access, use, disclosure, disruption, modification, or destruction, usually by enacting security controls.

- **Information Security Policy:** an aggregate of directives, regulations, rules, and practices that prescribe how an organization manages, protects, and distributes information.
- **Information System Management:** administering databases, network components, workstations, or servers — typically requiring privileged users' access.
- **Organization:** a federal Agency or, as appropriate, any of its operational elements.
- **Plan of Action and Milestones (POA&M):** plans of corrective actions that are designed to counter discovered risks and threats to the organization or organizational assets.
- **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.
- **Risk Assessment:** the process of identifying risks to Agency operations (including mission, functions, image, or reputation), Agency assets, individuals, other organizations, and the Nation arising through the operation of the information system. Part of risk management, synonymous with risk analysis, incorporates threat and vulnerability analyses, and considers mitigations provided by planned or in-place security controls.
- **Risk Management:** the process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes:
    - The performance of a risk assessment;
    - The implementation of a risk mitigation strategy; and
    - Employment of techniques and procedures for the continuous monitoring of the security state of the information system.
- **Security Categorization:** describes the potential adverse impacts to organizational operations, organizational assets, and individuals should the information and information system be compromised through a loss of confidentiality, integrity, or availability.
- **Security Controls:** safeguards or countermeasures that, when instituted, assist to avoid, counteract, or minimize security risks.
- **Security Metrics:** the measurement of the effectiveness of security controls put in place to secure organizational information and information systems.
- **Threat:** any circumstance or event with the potential to adversely impact Agency operations (including mission, functions, image, or reputation), Agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
- **Vulnerability:** weakness in an information system, system security procedures, internal controls, or implementation that could be exploited.

- **Vulnerability Assessment:** formal description and evaluation of vulnerabilities of an information system.

Abbreviations including acronyms are summarized in *Appendix: Acronyms & Abbreviations*.

10. WAIVERS

Waivers may be requested from the CIO by submitting a justification based on:

- substantive business case need(s)
- demonstration of, or a proposal for, establishment of adequate compensating controls that provide a suitable alternative to the mandated protection

The CIO may grant a waiver for sufficient reasons exercising judgment in the best interests of the Agency.

The SAISO and Director of OITO shall coordinate to maintain a central repository of all waivers.

11. MATERIAL SUPERSEDED

N/A

12. CONTACTS

For further information, please contact the Office of Environmental Information (OEI), Office of Information Security and Privacy (OISP).

Ann Dunkin
Chief Information Officer
U.S. Environmental Protection Agency

APPENDIX:
ACRONYMS & ABBREVIATIONS

AA	Assistant Administrator
CCP	Common Control Provider
CFO	Chief Financial Officer
CIO	Chief Information Officer
CSIRC	Computer Security Incident Response Capability
DHS	Department of Homeland Security
EPA	Environmental Protection Agency
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
HSPD	Homeland Security Presidential Directive
IMO	Information Management Officer
IO	Information Owner
IRMBC	Information Resource Management Branch Chief
ISO	Information Security Officer
ISSO	Information System Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
OEI	Office of Environmental Information
OISP	Office of Information Security and Privacy
OITO	Office of Information Technology Operations
OMB	Office of Management and Budget
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
POC	Point of Contact
PO/R	Program Office or Region
PM	Program Management
RA	Regional Administrator
SAISO	Senior Agency Information Security Officer
SBO	Senior Budget Officer
SIO	Senior Information Official
SM	Service Manager
SO	System Owner
SP	Special Publication
USC	United States Code