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

# Information Security – Roles and Responsibilities Procedures

## 1. PURPOSE

The purpose of this document is to ensure that the EPA roles are defined with specific responsibilities for each role and for people who have been assigned to the listed roles. The roles and responsibilities in this document shall be reviewed for each individual to comprehensively understand their role and specific responsibilities in their environmental context. This procedure amplifies the roles and responsibilities delineated in the EPA Information Security Policy.

## 2. SCOPE

These procedures cover all EPA information and information systems to include information andinformation systems used, managed, or operated by a contractor, another Agency, or other 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 EPA.

## 3. AUDIENCE

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

## 4. BACKGROUND

Pursuant to the Federal Information Security Management Act (FISMA) of 2002 and the Officeof Management and Budget (OMB) Circular A-130, Appendix III, Environmental Protection Agency (EPA) requires employees and contractors fulfilling roles with significant information security responsibilities to understand and have the capacity to carry out these responsibilities. In response to this requirement, EPA has developed a procedure defining each role and outlining necessary responsibilities to ensure the confidentiality, integrity, and availability of EPA's information and information systems.

## 5. AUTHORITY

- *Federal Information Security Management Act of 2002* (FISMA), Public Law 107-347 as amended
- Office of Management and Budget (OMB) Memorandum M-06-16, *Protection of Sensitive Agency Information*
- OMB Circular A-130, Management of Federal Information Resources, revised

- National Institute of Standards and Technology (NIST), Federal Information Processing Standards Publication (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006, as amended
- National Institute of Standards and Technology (NIST), Special Publication 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations, A System Life Cycle Approach for Security and Privacy*.
- EPA CIO 2150.5, *Information Security Policy*, and all subsequent updates or superseding directives

## 6. ROLES AND RESPONSIBILITIES

This section provides roles and responsibilities for personnel who have IT security or related governance responsibility for protecting the information and information systems they operate,manage and support. The National Institute of Standards and Technology (NIST) information security related publications will be a primary reference used to develop EPA procedures, standards, guidance and other directives in support of EPA policy. EPA directives will supplement, clarify, and implement NIST, OMB and other higher-level directives for EPA's systems, operations, and environments.

a) The **EPA Administrator** is responsible for:

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

2) Providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, ordestruction 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.

3) Ensuring that information security management processes are integrated with Agency strategic and operational planning processes.

4) Ensuring that Assistant Administrators (AAs), Regional Administrators (RAs) and other key officials provide information security for the information and information systems that support the operations and assets under their control.

5) Ensuring enforcement and compliance with FISMA and related information security directives.

6) Delegating to the Assistant Administrator, Office of Mission Support – Environmental Information/Chief Information Officer (CIO) the authority to ensure compliance with FISMA and related information security directives.

7) Ensuring EPA has trained personnel sufficient to assist in complying with

FISMA and other related information security directives.

8) Ensuring that the CIO, in coordination with AA, RAs and other key officials, reports annually the effectiveness of the EPA information security program, including progress of remedial actions, to the EPA Administrator, Congress, OMB, Department of Homeland Security (DHS) and other entities as required by law and Executive Branch direction.

9) Ensuring 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.

b) The **Chief Information Officer (CIO)** is responsible for:

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

2) Developing, documenting, implementing, and maintaining 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.

a) Developing, documenting, implementing, and maintaining Agency-wide, well-designed, well-managed continuous monitoring and standardized risk assessmentprocesses.

3) Developing, maintaining, and issuing Agency-wide information security policies, procedures, and control techniques to provide direction for implementing the requirements of the information security program.

4) Training and overseeing personnel with significant information security responsibilities with respect to such responsibilities.

5) Assisting senior Agency and other key officials with understanding and implementing their information security responsibilities.

6) Establishing minimum mandatory risk based technical, operational, and management information security control requirements for Agency information and information systems.

7) Reporting any compliance failure or policy violation directly to the appropriate AA or RA or other key officials for appropriate disciplinary and corrective actions.

8) Requiring any AA, RA or other key official who is so notified to report back to the CIO regarding what actions are to be taken in response to any compliance failure or policy violation reported by the CIO.

9) Ensuring EPA Senior Information Official (SIOs) and Information Security Officers (ISOs) comply with all EPA Information Security Program

requirements and ensuring that these staff members have all necessary authority and means to direct full compliance with such requirements.

10) Establishing the EPA National Rules of Behavior (NROB) for appropriate use and protection of the information and information systems which support EPA missions and functions.

11) Developing, implementing, and maintaining capabilities for detecting, reporting, and responding to information security incidents.

12) Designating a Chief Information Security Officer (CISO) whose primary duty is information security in carrying out the CIO responsibilities under EPA policy and relevant information security laws, Executive Branch policy, and other directives.

13) Ensuring that the CISO 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.

14) Ensuring that the CISO heads an office with the mission and resources required to administer the EPA Information Security Program functions, carry out the CIO responsibilities under EPA policy, and assist in ensuring Agency compliance with EPA policy.

15) Reporting 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.

16) Serving as the Risk Executive for the Agency's information security Risk Executive Function. As such, coordinating with the Risk Executive Group, Chief Information Security Officer (CISO), Senior Information Officials (SIOs), Information Management Officers (IMOs), Information Security Officers (ISOs), and System Owners (SOs) in governing risk.

17) Coordinating with AAs, RAs and other key officials for information systems' aspects of continuity of operations.

c) The **Chief Information Security Officer (CISO)** is responsible for:

1) Providing recommendations to the Risk Executive and Risk Executive Group.

2) Maintaining professional qualifications required to administer the functions of the EPAInformation Security Program and carry out the CIO responsibilities under EPA policy and relevant information security laws, Executive Branch policy, and other directives.

3) Carrying out the CIO responsibilities under EPA policy and relevant information security laws, Executive Branch policy, and other directives.

a) Developing, documenting, implementing and maintaining an Agency-wide information security program to protect EPA information and information systems.

   (i) Developing documenting, implementing, and maintaining Agency-wide, well- designed, well-managed continuous monitoring and standardized risk assessment processes.

b) Ensuring 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.

c) Developing, maintaining and distributing Agency-wide information security policies, procedures, and control techniques to provide direction for implementing the requirements of the information security program.

d) Assisting senior Agency and other key officials with understanding and implementinginformation security responsibilities that fall within their realm of oversight.

e) Establishing minimum, mandatory risk based technical, operational, and management information security control requirements for the Agency information security program, information, and information systems.

f) Reporting compliance failures and policy violation directly to the appropriate organizational officials for appropriate disciplinary and corrective actions.

g) Requiring organizational officials informed of compliance failures and policy violations to report the status of disciplinary and corrective actions.

h) Ensuring SIOs, IMOs, and ISOs comply with all information security program requirements, and that these personnel have all necessary authority and means todirect full compliance with such requirements.

i) Reporting annually, in coordination with other Agency officials, the effectiveness ofthe information security program, and the progress of remedial actions, to the EPAAdministrator.

j) Developing, implementing, and maintaining security authorization and reporting capabilities, including the Agency security information repository[1], as required by the information security program, and applicable policy and procedures.

k) Developing and maintaining role-based training, education and credentialing requirements to ensure personnel with significant

[1] *Xacta is the current enterprise tool for recording and maintaining a system inventory, reporting authorizations, storing information security documents and related system information, and managing POA&Ms.*

information security responsibilities receive adequate training with respect to such responsibilities.

(i) Making final determination for acceptability of training to meet role-based training, education and credentialing requirements.

(ii) Making final determination for acceptability of credentials, e.g., (ISC)[2], ISACA, SANS, NSA IEM, etc., to meet role-based credentialing requirements.

l) Managing the user awareness program and developing and maintaining user awareness content.

m) Developing and maintaining NROB for appropriate use and protection of information and information systems which support EPA missions and functions.

n) Coordinating with the Director, Office of Technology Operations and Planning (OPTOP) in delivering awareness, training, education, and NROB content and tracking completion.

o) Coordinating with the OITO Director to ensure the Agency can adequately detect, respond, and report information security incidents.

p) Coordinating with independent auditors, audit coordinators, SIOs, IMOs, ISOs and other key officials to manage audits and audit responses.

q) Coordinating with independent auditors, audit coordinators, SIOs, IMOs, ISOs and other key officials in ensuring FISMA monthly, quarterly and annual reports, as required by OMB, are produced and submitted for approval in a timely fashion. Validating report content and uploading reports to the federal reporting mechanism[2].

4) Providing guidance to EPA ISOs. Leading periodic meetings to disseminate information, discuss and resolve issues, and develop solutions and courses of action for implementing the EPA Information Security Program objectives.

5) Implementing and leading the Quality and Information Council's (QIC) Quality Technology Subcommittee (QTS) Agency Information Security Program Work Group (AISP-WG). Coordinating with the OITO Director as a co-executive sponsor for the AISP-WG.

6) Periodically providing relevant and up-to-date security information to personnel with significant information security responsibilities via standard, internal communication mechanisms.

7) Coordinating with EPA Office of Inspector General personnel to ensure the EPA information security program and protection measures are compliant with

[2] *Cyberscope is the current tool used to report Agency information security status*

FISMA and related information security directives.

8) Coordinating with the EPA Privacy Officer during security incidents involving personally identifiable information and in identifying EPA Information Security Program related controls and processes that can support EPA's Privacy Program objectives

9) Coordinating with EPA Office of Administration and Resource Management (OARM) personnel for physical security requirements.

10) Coordinating with EPA Office of Homeland Security (OHS) personnel for international travel requirements, threat analysis and identification, and information security incidents.

11) Coordinating with EPA Office of the Chief Financial Officer personnel for Federal Managers Financial Integrity Act annual audits.

12) Coordinating with the Director, Office of Technology Operations and Planning on information security related Capital Planning and Investment Control processes.

d) **Assistant Administrators, Regional Administrators, and other key officials (e.g., Principal Deputy Assistant Administrators, Deputy Assistant Administrators, Deputy Regional Administrators, Assistant Regional Administrators, and Office Directors)** are responsible for:

1) Implementing policies, procedures, control techniques and processes identified in the Agency information security program that comprise activities that are under their day-to- day operational control or supervision.

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

a) Issuing local information security procedures and control techniques for local systems and operations as necessary to support and implement the Agency information security program policies, procedures, and control techniques.

b) Coordinating with the CIO, Risk Executive, Risk Executive Group, CISO and othersinvolved with securing Agency information and systems to ensure risks are managed to an acceptable level.

c) Executing the appropriate security controls in response to Computer Security Incident Response Capability (CSIRC) notifications. Such notifications shall be complied with immediately.

d) Ensuring all EPA information and information system users within their organizations successfully complete information security awareness prior to

initial access to EPA systems and information and at least annually thereafter to maintain access.

e) Ensuring all employees within their organizations designated as having significant information security responsibilities complete role-based information security trainingand education and obtain credentials as defined under the EPA Information Security Program to maintain access and perform in identified roles.

f) Coordinating with the CISO in responding to information security data calls, auditrequests, and reporting.

3) Ensuring 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 CSIRC notification.

4) Enforcing and ensuring the NROB, and additional system specific rules of behavior where applicable, are reviewed and signed or acknowledged electronically or manually prior to being granted access to EPA information and information systems and annually thereafter to maintain access.

5) Coordinating with the EPA's Office of Administration and Resources Management (OARM) Security Management Division for physical security requirements, Assistant Administrators, Regional Administrators, or as delegated, Deputy Assistant Administrators or Deputy Region Administrators shall designate in writing Information Security Officers.

e) The **Risk Executive** is responsible for:

1) Coordinating with the Risk Executive Group (REG) to ensure:

a) Risk-related considerations for individual information systems, to include authorization decisions, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the Agency in carrying out its core missions and business functions.

b) Information system-related security risks management is consistent across the organization, reflects organizational risk tolerance, and is considered along with other types of risks in order to ensure mission/business success.

2) Disseminating resultant risk direction to SIOs, IMOs, ISOs, and system and information owners.

f) The **Risk Executive Group (REG)** is responsible for:

1) Coordinating with the senior leadership, mission and business managers, system and information owners and others to provide recommendations to the Risk Executive for making risk-related decisions and providing risk-related direction to SIOs, IMOs, ISOs, and system and information owners.

g) **Senior Information Officials (SIO)** are responsible for:

1) Ensuring effective processes and procedures and other directives as necessary are established to implement the policies, procedures, control techniques, and other countermeasures identified under the EPA Information Security Program and enforced within their respective offices or regions.

2) Carrying out the duties of the Mission or Business Owner for their office or region.

3) Carrying out the duties of the Authorizing Official (AO) for their office or region.

a) Making risk-based system authorization decisions derived from information contained in the authorization package.

b) Reviewing authorization packages.

i. Approving authorization packages.

1) Signing or acknowledging electronically or manually an authorization to operate (ATO)[3] documenting the decision to allow operation of a particular system and formally assuming responsibility and accountability of its security and operation at an acceptable level of risk to Agency operations and assets, individuals, other organizations and the Nation.

2) Signing or acknowledging an ATO also documents the approval of the associated authorization package.

3) Approving system security plans, memorandums of agreement or understanding, and plans of action and milestones.

ii. Denying authorization to operate or halting system operations if risks are unacceptable.

1) Documenting in writing or electronically the decision to deny authorization to operate or halt system operations.

iii. Determining whether significant changes in the information systems or environments of operation require reauthorization.

3) When delegating AO duties, designating in writing, as needed, an Authorizing Official Designated Representative (AODR) to carry out those duties.

[3] *Authorization to Operate is used to represent other allowable authorizations, such as an Authorization to Test, in this document.*

*Note: "Interim Authorization to Operate" is not recognized by OMB as an acceptable determination and is not used in EPA*

a) Individuals designated as an Information Management Officer (IMO) have been delegated AODR type responsibilities and further designation is not required for IMOs serving in the AODR role.

b) The SIO cannot delegate to the AODR or any other role the authorization decision or the signing or acknowledging electronically or manually an ATO. The decision to allow operation of a particular system and formally assuming responsibility and accountability of its security and operation at an acceptable level of risk to Agency operations and assets, individuals, other organizations and the Nation cannot be delegated.

4) Coordinating with the CIO, Risk Executive, Risk Executive Group, CISO, and AODRs, ISOs and others involved with securing Agency information and systems to ensure they are adequately secure and risks are managed to an acceptable level.

5) Ensuring system controls are continuously monitored, operating as expected and adequately protecting information.

a) Periodically reviewing system and control statuses to properly manage risks and ensure systems and information are adequately protected.

b) Taking appropriate action before risks become unacceptable and controls are not providing adequate protection.

6) Coordinating with the CISO in responding to information security data calls, audit requests, and reporting.

h) **Authorizing Official Designated Representatives (AODR)** are responsible for:

1) Carrying out the duties of the AO as assigned.

a) An AODR cannot be assigned nor carry out duties that accept risk to organizational operations and assets, individuals, other organizations, and the Nation.

i. The AODR cannot make the authorization decision or sign or acknowledge electronically or manually an authorization to operate (ATO).

2) Coordinating and conducting the required day-to-day activities associated with the authorization process and ensuring risks are managed properly and systems and information are adequately protected.

i) **Information Security Officers (ISO)** are responsible for:

1) Supporting the AA or RA by managing activities identified under the EPA Information Security Program and ensuring protection measures are compliant with FISMA and related information security directives for the information, information systems, and services for their office or region to include but not limited to:

a) Coordinating with the CISO in developing, documenting, implementing, and maintaining an office or region and Agency-wide information security programs to protect EPA information and information systems.

b) Coordinating with the CISO in responding to information security data calls, audit requests, and reporting.

c) Implementing policies, procedures, and control techniques identified in the Agency information security program.

d) Providing guidance on their roles and responsibilities and Agency information security program requirements to ISSOs, system administrators, and others with significant security responsibilities.

e) Tracking and ensuring all EPA information and 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. Ensuring access is removed for users who do not successfully complete awareness training.

f) Tracking and ensuring 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) Making determination for acceptability of training to meet role based training, education, and credentialing requirements in accordance with information security training and education program requirements. Referring to CISO for final determination as necessary.

h) Enforcing and ensuring the NROB, and additional system specific rules of behavior where applicable, are reviewed and signed or acknowledged electronically or manually prior to being granted access to EPA information and information systems and annually thereafter to maintain access. Ensuring access is removed for users who do not do so.

2) Supporting the SIO in ensuring effective processes and procedures and other directives are established as necessary to implement the policies, procedures, control techniques, and other countermeasures identified under the EPA Information Security Program and enforced for their office or region by taking actions to include but not limited to:

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

b) Reviewing periodically the Agency information security system inventory tool and ensuring systems are reported accurately and completely.

c) Reviewing periodically the Agency information security information repository and ensuring all system information security information, such as plans of actions and milestones, system security plans, and security assessment reports, are entered and maintained accurately and up to date.

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

e) Monitoring POA&Ms to ensure weakness remediation and mitigation are managed and actions are documented properly.

f) Coordinating and liaising with local, other EPA, and external personnel for system and information security management, operations and control monitoring, audits, assessments, incident response, and law enforcement investigations.

g) Coordinating with CSIRC as a first responder for incidents affecting the assigned organization's information, systems or personnel.

h) Providing expert advice in developing and updating enterprise and local information security documents to include policy, procedures, standards and guides.

i) Coordinating with and supporting the IMO and AODR in implementing EPA Information Security Program requirements.

3) Supporting system owners, information owners, and service managers 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 adequately protect supported information within acceptable risks by taking actions to include but not limited to:

a) Providing expert advice in:

(i) developing and updating mandatory configurations for information technology products and solutions used by EPA;

(ii) determining local controls to ensure compatibility and interoperability with enterprise tools and controls;

(iii) implementing, operating, and maintaining enterprise tools and controls;

(iv) ensuring information and systems are properly categorized;

(v) defining, developing, documenting, implementing, assessing, and monitoring all controls to include common and hybrid controls;

(vi) conducting impact analyses for proposed or actual changes to systems or their operational environments; and

4) Developing and implementing system decommissioning and information disposal strategies.

j) **Information Management Officers (IMO)** are responsible for:

1) Supporting the SIO in implementing the SIO's information technology and information management functions and responsibilities related to information security.

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

b) Developing and issuing local information security procedures, control techniques and processes for local systems and operations as necessary to support and implement the Agency information security program policies, procedures, and control techniques.

c) Executing the appropriate security controls and processes commensurate with responding to a CSIRC security notification. Such notifications shall be complied with immediately.

d) Ensuring 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 CSIRC notification.

e) Ensuring all EPA information and 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.

f) Enforcing and ensuring the NROB, and additional system specific rules of behavior where applicable, are reviewed and signed or acknowledged electronically or manually prior to being granted access to EPA information and information systems and annually thereafter to maintain access.

g) Ensuring all employees within their organizations designated as having significant information security responsibilities complete role-based information security training as defined under the EPA Information Security Program.

h) Coordinating with the CISO in responding to information security data calls, audit requests, and reporting.

2) Coordinating with the CIO, Risk Executive, Risk Executive Group, CISO, and ISOs, system and information owners and others involved with securing Agency

information and systems to ensure they are adequately secure and risks are managed to an acceptable level.

k) **Directors, Office of Information Technology Operations (OITO) and Office of Mission Support – Environmental Information** are responsible for:

1) Developing, maintaining and issuing 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 CISO issued policies, procedures and control techniques.

2) Implementing, operating, and maintaining enterprise tools and controls required to implement the Agency information security program policies, procedures, and control techniques.

3) Defining, implementing, and coordinating processes for use and maintenance of enterprise tools and controls.

4) Coordinating with program offices and regions and other entities as necessary on the implementation, operation, and maintenance of enterprise tools, controls, and processes.

5) Ensuring the Chief Enterprise Architect supports developing, maintaining, and implementing the Agency's Information Security Architecture.

6) Monitoring for and notifying the CIO, CISO, SIO's and other personnel as appropriateof potential and actual threats to Agency information system resources.

7) Verifying and enforcing that only those information systems having approved authorizations to operate or test are attached to the EPA network.

8) Providing security awareness and role-based training delivery mechanisms and relatedsupport.

9) Implementing and managing enterprise capabilities[4] for detecting, reporting, and responding to security incidents where (a) risks are mitigated before substantial damage is done, (b) the United States Computer Emergency Readiness Team (US-CERT) is notified and consulted, (c) law enforcement agencies and the EPA Office of Inspector General, and any other Agency or office in accordance with law or as directed by the President is notified and consulted as appropriate, and (d) the CIO and CISO and ISOs, SOs, IOs, and others are notified and coordinated with.

10) Coordinating with program offices, regions and other entities as appropriate when they implement local controls to ensure compatibility and interoperability with

[4] *EPA's implementation of these capabilities is called the Computer Security Incident Response Capability (CSIRC).*

enterprise tools, controls and processes.

11) Leading the development, documentation, and maintenance of mandatory configurations for information technology products and solutions used by EPA.

12) Reviewing and updating the enterprise baseline configurations periodically.

13) Establishing and managing enterprise configuration change management capabilities for all information technology.

14) Coordinating with the CISO as a co-executive sponsor for the AISP-WG and providing support for the AISP-WG.

15) Coordinating with OHS personnel for threat analysis and identification and information security incidents.

16) Coordinating with the OARM personnel for physical security requirements.

l) **Assistant Administrator, Office of Homeland Security (OHS)** is responsible for:

1) Leading all activities at EPA related to the notification and dissemination of national security intelligence, terrorism information, and other sensitive information. Developing and implementing the Agency's policies and procedures for reviewing, analyzing and disseminating intelligence and sensitive information as described in EPA's Intelligence Notification and Dissemination Policy and the Standard Operating Procedures of Intelligence and Other Sensitive Information.

2) Providing regularly scheduled intelligence briefings to the Administrator, Deputy Administrator, Chief of Staff, and other senior EPA managers.

3) Serving as the lead for providing national security intelligence briefings to all EPA personnel.

4) Serving as the principal EPA liaison to the U.S. Intelligence Community (IC). This includes coordinating requests from the IC for EPA assistance (e.g. evaluating a particular piece of intelligence or sensitive information from a scientific or technical perspective), or requests from EPA for IC assistance.

a) Coordinating with the OITO Director and CISO on incident response activities by evaluating and providing intelligence information.

5) Coordinating with the CISO for international travel requirements.

m) **System Owners (SO)** are responsible for:

1) Implementing policies, procedures, and control techniques identified in the Agency information security program.

a) Coordinating with the CSIRC.

b) Assigning an ISSO in writing for each system.

c) Developing and implementing procedures, control techniques, and other countermeasures as necessary to support and implement Agency information security program requirements.

2) Coordinating with the CIO, CISO, information owners, other system owners, and service managers regarding EPA Information Security Program requirements for assigned systems during their entire lifecycles.

3) Developing, maintaining, and providing information security documents as required under the EPA Information Security Program for assigned systems.

a) Maintaining accurately and up to date all system information security information, such as plans of actions and milestones, system security plans, and security assessment reports, in the Agency information security information repository[3].

b) Reporting systems in the Agency information security system inventory tool[5] and maintaining system information accurately and up to date.

4) Coordinating with information owners for deciding who has access (and with what types of privileges or access rights), enforcing access, and ensuring system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior) for assigned systems.

5) Coordinating with information owners and service managers for determining if additional rules of behavior are needed beyond those provided in the NROB for particular systems. If additional rules of behavior are needed, SOs will coordinate with information owners and service managers to establish and publish the additional rules of behavior.

6) Coordinating with the CIO, CISO, common control providers, information owners, and service managers regarding information security requirements and determining and carrying out responsibilities for defining, developing, documenting, implementing, assessing, and monitoring all controls to include common and hybrid controls.

7) Obtaining authorization to operate or authorization to test from the appropriate SIO prior to operational use or testing in an operational environment of any system.

a) Coordinating with ISSOs, ISOs, IMOs, and AODRs to assemble security authorization packages.

[5] *Xacta is the official enterprise tool and repository for recording and maintaining a system inventory for FISMAreporting and compliance purposes, recording and reporting authorizations, storing all information security documents and related system information, and managing POA&Ms. Xacta is the authoritative source for information security related information for all systems whether internally or externally managed*

8) Configuring, continuously monitoring, and maintaining systems to adequately protect information stored, processed, or transmitted within acceptable risks.

   a) Coordinating with information owners to ensure systems are properly categorized according to information categorizations.

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

   c) Deploying and operating systems according to the security requirements documented in security plans.

   d) Assessing all controls prior to systems becoming operational and minimally a subset of all controls annually thereafter. Assessing core controls annually as part of the subset of controls for annual assessment. Ensuring control assessments are conducted by third party control assessors for moderate and high categorized systems. Obtaining security assessment reports from assessors.

   e) Developing and managing plans of actions and milestones for discovered weaknesses.

      (i) Conducting remediation actions for discovered weaknesses based on risk decisions. Documenting risk decisions regarding discovered weaknesses to include transfer and acceptance.

   f) Conducting impact analyses for proposed or actual changes to systems or their operational environments.

   g) Developing and implementing system decommissioning strategies to properly dispose of systems. Coordinating with information owners to ensure resident information is properly disposed of and actions are included in the decommissioning strategy.

   h) Coordinating with the OITO Director to develop, document, and maintain mandatory configurations for information technology products and solutions used by EPA.

   i) Implementing mandatory configurations for information technology products and solutions used by EPA.

   j) Coordinating with the OITO Director to establish, manage and use enterprise configuration change management capabilities for all information technology used by EPA.

   k) Coordinating with the OITO Director for implementing local controls to ensure compatibility and interoperability with enterprise tools and controls.

l) Coordinating with the OITO Director for implementing, operating, and maintaining enterprise tools and controls.

9) Coordinating with the CISO in responding to information security data calls, audit requests, and reporting.

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

n) **Service Managers (SM)** are responsible for:

1) Implementing policies, procedures, and control techniques identified in the Agency information security program.

a) Coordinating with the CSIRC for enterprise services.

b) Assigning an ISSO in writing for each enterprise solution obtained.

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

2) Coordinating with the CIO, information owners, system owners, other service managers and service providers, e.g., cloud services, regarding EPA Information Security Program requirements for assigned services during their entire lifecycles.

3) Coordinating with information owners for deciding who has access to the service (and with what types of privileges or access rights) and ensuring service users and support personnel receive the requisite security training (e.g., instruction in rules of behavior).

4) Coordinating with information owners for determining 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 will coordinate with information owners to establish and publish the additional rules of behavior.

5) Coordinating with the CIO, common control providers, information owners, system owners, other service managers and service providers regarding information security requirements and determining and carrying out responsibilities for defining, developing, documenting, implementing, assessing, and monitoring common and hybrid controls.

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

7) Coordinating with IOs to ensure service providers' systems supporting non-enterprise services are configured, monitored, and maintained to adequately

protect supported information stored, processed, or transmitted within acceptable risks.

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

9) Following Federal Risk and Authorization Management Program (FedRAMP) requirements.

    a) Obtaining authorizations to operate or authorizations to test from the appropriate SIO prior to operational use or testing of any service for enterprise services.

        (i) Coordinating with ISSOs, ISOs and IMOs to assemble security authorization packages.

    b) Developing, maintaining, and providing information security documents as required under the EPA Information Security Program for enterprise services.

        (i) Maintaining accurately and up to date all system information security information, such as plans of actions and milestones, system security plans, and security assessment reports, in the Agency information security information repository.

        (ii) Reporting systems in the Agency information security system inventory tool and maintaining system information accurately and up to date.

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

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

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

13) Ensuring all controls are assessed prior to systems becoming operational and minimally a subset of all controls is assessed annually thereafter for enterprise services. Ensuring core controls are assessed annually as part of the subset of controls for annual assessments. Ensuring control assessments are conducted by third party control assessors for moderate and high categorized systems and obtaining security assessment reports from assessors.

14) Developing and managing and ensuring service providers develop and manage plans of actions and milestones for discovered weaknesses for enterprise services.

a) Conducting or ensuring service providers conduct remediation actions for discovered control weaknesses for enterprise services.

15) Conducting or ensuring service providers conduct impact analyses for proposed or actual changes to systems or their operational environments for enterprise services.

16) Developing and implementing or ensuring service providers develop and implement system decommissioning strategies to properly dispose of systems for enterprise services. Coordinating with information owners to ensure resident information is properly disposed of is included in the decommissioning strategy.

17) Ensuring service providers implement mandatory configurations for information technology products and services used by EPA for enterprise services.

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

19) Coordinating with the OITO Director and service providers for service providers implementing controls to ensure compatibility and interoperability with enterprise tools and controls for enterprise services.

20) Coordinating with the OITO Director for implementing, operating, and maintaining enterprise tools and controls for enterprise services.

21) Coordinating with the CISO in responding to information security data calls, audit requests, and reporting.

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

o) **Information Owners (IO)** are responsible for:

1) Implementing policies, procedures, and control techniques identified in the Agency information security program.

a) Coordinating with the CSIRC.

b) Assigning an ISSO in writing for each non-enterprise service obtained.

(i) Assignment of ISSOs by IOs is not required for services obtained as enterprise solutions.

c) Ensuring procedures, control techniques, and other countermeasures as necessary to support and implement Agency information security program requirements are implemented for non-enterprise services obtained.

2) Providing assistance to the CIO, CISO, system owners, common control providers, and service managers regarding the information security requirements

and appropriate security controls for the supporting information systems for the lifecycle of the information for which the IO is responsible.

a) Coordinating with system owners, common control providers, and service managers providing information as needed for developing, maintaining, and providing information security documents as required under the EPA Information Security Program.

b) Categorizing information and providing results to SOs, service managers, common control providers, and service providers. Coordinating with SOs, service managers, common control providers, and service providers to ensure supporting systems are properly categorized according to information categorization.

c) Coordinating with SOs, common control providers, service managers, and service providers to identify controls required to adequately protect information stored, processed, or transmitted by supporting systems. Identifying and providing information to SOs, common control providers, service managers, and service providers if additional or more stringent controls than those identified in the set of baseline controls are required according to risk analyses.

d) Verifying with SOs, common control providers and service managers to ensure systems used to store, process, or transmit information have and maintain current authorizations to operate or authorizations to test from the appropriate SIO prior to operational use or testing in an operational environment of any system.

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

4) Ensuring terms of service and other contractual agreements satisfy the security and privacy requirements applicable to EPA information systems and information for services for non-enterprise services obtained.

5) Following Federal Risk and Authorization Management Program (FedRAMP) requirements.

a) Obtaining authorization to operate or authorization to test from the appropriate SIO prior to operational use or testing in an operational environment for any non- enterprise service obtained.

b) Developing, maintaining, and providing information security documents as required under the EPA Information Security Program for non-enterprise services obtained.

(i) Maintaining accurately and up to date all system information 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.

a) Reporting systems in the Agency information security system inventory tool and maintaining system information accurately and up to date for non-enterprise services obtained.

(i) Coordinating with ISSOs, ISOs, IMOs, and AODRs to assemble security authorization packages.

6) Ensuring service provides deploy and operate systems according to the security requirements documented in security plans.

7) Ensuring all controls are assessed for systems supporting non-enterprise services obtained prior to using service and minimally a subset of all controls is assessed annually thereafter. Ensuring core controls are assessed annually as part of the subset of controls for annual assessments. Ensuring control assessments are conducted by third party control assessors for moderate and high categorized information and obtaining security assessment reports from assessors.

8) Developing and managing and ensuring service providers develop and manage plans of actions and milestones for discovered weaknesses for non-enterprise services obtained.

a) Conducting or ensuring service providers conduct remediation actions for discovered control weaknesses for non-enterprise service obtained.

9) Conducting or ensuring service providers conduct impact analyses for proposed or actual changes to systems or their operational environments for non-enterprise services obtained.

10) Developing and implementing or ensuring service providers develop and implement system decommissioning strategies to properly dispose of systems and resident information for non-enterprise services obtained.

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

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

13) Coordinating with the OITO Director and service providers for service providers implementing controls to ensure compatibility and interoperability with enterprise tools and controls for enterprise services.

14) Coordinating with the CISO in responding to information security data calls, audit requests, and reporting.

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

16) Approving who has access to a system or service containing information for which the IO is responsible, to include types of privileges and access rights.

    a) Approving and providing information to SOs, common control providers, service managers, and service providers on who has access (and with what types of privileges or access rights) and ensuring system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior) for assigned systems.

17) Enforcing and ensuring the EPA NROB, and additional rules of behavior for particular systems, if established, are signed or acknowledged electronically or manually annually by all information users that support the operations and assets of EPA for information for which the IO is responsible.

    a) Tracking rules are signed or acknowledged by all users.

    b) Ensuring accesses to systems are removed for users that do not sign or acknowledge rules.

18) Determining and providing information to SOs and service managers on additional rules of behavior needed beyond those provided in the national rules of behavior for particular systems. If additional rules of behavior are needed, IO's will coordinate with SOs and service managers to establish and publish the additional rules of behavior.

19) Coordinating with the CIO, CISO, common control providers, SOs, service managers, and service providers regarding information security requirements and determining and carrying out responsibilities for defining, developing, documenting, implementing, assessing, and monitoring all controls to include common and hybrid controls.

p) **Information System Security Officers (ISSO)** are responsible for:

1) Supporting the SIO, SO, SM, IO and ISO in managing and implementing the activities, processes, policies, procedures, control techniques, and other countermeasures identified under the EPA Information Security Program and ensuring protection measures are compliant with FISMA and related information security directives for the information, information system, and service assigned by taking actions to include but not limited to:

    a) Ensuring the day-to-day security operations of an information system, including verifying that security controls, technical and otherwise, are functioning as intended.

    b) Developing and maintaining 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.

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

d) Reporting systems in the Agency information security system inventory tool and maintaining current and accurate information.

e) Entering into the Agency information security information repository and all system information security information, such as plans of actions and milestones, system security plans, and security assessment reports, and maintaining current and accurate information.

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

g) Responding to information security data calls, audit requests, and reporting.

h) Providing expert advice in:

(i) developing and updating mandatory configurations for information technology products and solutions used by EPA;

(ii) determining local controls to ensure compatibility and interoperability with enterprise tools and controls;

(iii) implementing, operating, and maintaining enterprise tools and controls; and

(iv) ensuring information and systems are properly categorized.

2) Serving as a principal advisor on all matters, technical and otherwise, involving the security of information, information system, or services assigned.

3) Implementing policies, procedures, and control techniques identified in the Agency information security program.

q) **Managers and Supervisors** are responsible for:

1) Ensuring policies, procedures, controls, and other countermeasures identified in the Agency information security program that comprise activities under their day-to-day operational control or supervision are implemented.

2) Executing the appropriate security controls commensurate with responding to a CSIRC security notification. Such notifications shall be complied with immediately.

3) Ensuring all employees 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 CSIRC notification.

4) Ensuring all employees designated as having significant information security responsibilities complete role based training, education, and credentialing requirements in accordance with information security training and education program requirements. Removing employees from such roles until requirements are met.

5) Ensuring that users successfully complete information security awareness training prior to initial access to EPA systems and information and at least annually thereafter to maintain access. Ensuring access is removed for users who do not successfully complete awareness training.

6) Ensuring that the NROB are reviewed and signed or acknowledged electronically or manually annually by all information and information system users who support the operations and assets for which EPA is responsible. Ensuring access is removed for users who do not do so.

r) **Common Control Providers (CCP)** are responsible for:

1) Documenting common controls in a security plan.

2) Coordinating with the CIO, CISO, information owners, and service managers regarding information security requirements and determining and carrying out responsibilities for defining, developing, documenting, implementing, assessing, and monitoring all controls to include common and hybrid controls.

3) Developing, implementing, assessing, configuring, continuously monitoring, and maintaining common controls to adequately protect information stored, processed, or transmitted within acceptable risks.

a) Coordinating with information owners to ensure systems are properly categorized according to information categorizations.

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

c) Deploying and operating systems according to the security requirements documented in security plans.

d) Assessing all controls prior to systems becoming operational and minimally a subset of all controls annually thereafter. Assessing core controls annually as part of the subset of controls for annual assessment. Ensuring control assessments are conducted by third party control assessors for moderate and high categorized systems. Obtaining security assessment reports from assessors.

e) Developing and managing plans of actions and milestones for discovered weaknesses.

(i) Conducting remediation actions for discovered weaknesses based on risk decisions. Documenting risk decisions regarding discovered weaknesses to include transfer and acceptance.

f) Conducting impact analyses for proposed or actual changes to systems or their operational environments.

g) Developing and implementing system decommissioning strategies to properly dispose of systems. Coordinating with information owners to ensure resident information is properly disposed of and actions are included in the decommissioning strategy.

h) Coordinating with the OITO Director to develop, document, and maintain mandatory configurations for information technology products and solutions used by EPA.

i) Implementing mandatory configurations for information technology products and solutions used by EPA.

j) Coordinating with the OITO Director to establish, manage and use enterprise configuration change management capabilities for all information technology used by EPA.

k) Coordinating with the OITO Director for implementing common controls to ensure compatibility and interoperability with enterprise tools and controls.

l) Coordinating with the OITO Director for implementing, operating, and maintaining enterprise tools and controls.

4) Coordinating with the CISO in responding to information security data calls, audit requests, and reporting.

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

6) Providing security plans, security assessment reports, and plans of action and milestones to information owners and system owners inheriting common controls.

s) **Security Control Assessors (SCA)** are responsible for:

1) Conducting objective and comprehensive assessments of management, operational, and technical controls implemented within EPA information systems in support of the security authorization and continuous monitoring processes.
2) Identifying weaknesses or deficiencies in EPA information systems related to security control design, implementation, and maintenance.

3) Providing a Security Assessment Report (SAR) to SOs, IOs, SMs, ISOs, and ISSOs that accurately reflects the status of security controls that have been assessed.

t) **The Inspector General (IG**) is responsible for:

1) Conducting an annual audit of the EPA information security program. Ensuring annual independent evaluation of the Agency information security program and practices to determine the effectiveness of such program and practices.

2) Reporting annually audit results to the EPA Administrator.

3) Conducting information security related criminal investigations when warranted.

4) Coordinating with the CSIRC, CIO, and CISO for information security related investigations.

u) The **Computer Security Incident Response Capability (CSIRC)** is responsible for:

1) Developing, maintaining, and implementing procedures, standards, and guides as necessary to implement the enterprise information security detection, report, and response team.

2) Ensuring prompt response and documentation of all information technology related privacy and information security incidents.

3) Ensuring threat and incident information reported, communicated, and used to inform the Agency's information technology security risk management awareness and training, privacy, and physical security management programs.

4) Cooperating with internal and external security, Law Enforcement and Counterintelligence authorities when warranted.

v) The **Network Security Operation Center (NSOC)** is responsible for:

1) Developing, maintaining, and implementing procedures, standards, and guides as necessary to implement EPA-wide information security policies, procedures, and control techniques to develop and provide situational awareness of Agency systems' security to Agency personnel.

2) Coordinating with internal and external personnel for configuring and monitoring systems, providing visibility into, alerting on, and analyzing monitored information.

w) The **Privacy Officer (PO)** is responsible for:

1) Providing privacy management and policy guidance.

2) Developing Agency-level privacy policies, procedures, standards, and guidelines.

3) Providing oversight of information system design, implementation, and management activities to ensure all privacy-related, statutory, regulatory and EPA requirements are met.

4) Implementing privacy policy changes in a timely manner based on the results of oversight activities, changes in regulations, and changes in roles and responsibilities.

5) Reviewing Privacy Impact Assessments (PIA) as required by the E-Government Act.

6) Ensuring programmatic and technical privacy controls are implemented.

7) Reporting privacy data in support of quarterly and annual FISMA reports.

8) Coordinating with the CISO during security incidents involving personally identifiable information (PII) and in identifying EPA Information Security Program related controls and processes that can support EPA's Privacy Program objectives.

x) **Acquisition Officials** are responsible for:

1) Ensuring contracts contain information security clauses and language for safeguarding Agency interests through its contractual relationships.

y) **Contracting Officers (CO)** are responsible for:

1) Ensuring contracts contain information security clauses and language for safeguarding Agency interests through its contractual relationships.

2) Ensuring, with the assistance of the Contracting Officer Representative, that products and services meet all Agency information security requirements.

z) **Contracting Officer's Representatives (COR)** are responsible for:

1) Ensuring contracts contain information security clauses and language for safeguarding Agency interests through its contractual relationships.

2) Assisting the Contracting Officer in the technical monitoring and administration of contract.

3) Ensuring, with the assistance of Agency technical staff, that products and services meet all Agency information security requirements.

aa) The **Chief Enterprise Architect** is responsible for:

1) Coordinate with the CISO to develop and implement the Agency's information security architecture.

2) Facilitating the integration of information security into all layers of enterprise architecture to ensure Agency implementation of security solutions.

bb) **Senior Resource Officials (SRO)** are responsible for:

1) Managing resources effectively, ensuring appropriate resources are available to meet information security requirements.

cc) **EPA Information and Information System Users** (i.e., employees, contractors, grantees, and others that support the operations and assets of EPA) are responsible for:

1) Complying with policies, procedures, and control techniques identified in the Agency information security program.

2) Complying with local information security procedures and control techniques.

3) Complying with CSIRC security notifications. Such notifications shall be complied with immediately.

4) Taking 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 CSIRC notification.

5) Reporting confirmed or suspected information security incidents and violations to the EPA Call Center and other designated entities.

6) Successfully complete information security awareness training prior to initial access to EPA systems and information and at least annually thereafter to maintain access.

7) Signing or acknowledging electronically or manually annually the NROB, and additional rules of behavior for particular systems if established, to maintain access.

dd) **Employees Designated As Having Significant Information Security Responsibilities** are responsible for:

1) Implementing policies, procedures, and control techniques identified in the Agency information security program.

2) Completing role-based information security training and credentialing as defined under the EPA Information Security Program.

## 7. RELATED INFORMATION

- NIST Special Publications – 800 series
- NIST Federal Information Processing Standards

- Related IT/IM policy, procedures, standards and guidance are available on OMS-EI's Policy Resources website.
- *Senior Information Officials*, CIO 2102, July 7, 2005
- *Senior Resource Officials and Resource Management Committee,* EPA Order 1130.2A, November 6, 1995
- *Intelligence Operations*¸ EPA Order 3220, December 30, 2008

## 8. DEFINITIONS

- Authorization (to operate) – The official management decision given by a senior Agency official to authorize operation of an information system and to explicitly accept the risk to Agency operations (including mission, functions, image, or reputation), Agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

- Authorizing Official – A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to Agency operations (including mission, function, image, or reputation), Agency assets, or individuals.

- Availability – Ensuring timely and reliable access to and use of information.

- Common Control Provider – Agency official responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inherited by information systems).

- Confidentiality – Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

- Information – Any communication or representation of knowledge such as facts, data, or opinions in any medium – including paper and electronic – or form – including textual, numerical, graphic, cartographic, narrative, or audiovisual.

- Information Owner – Agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, or disposal.

- Information Resources – Information in any form or media and its related resources, such as personnel, equipment, funds, and information technology.

- Information Security – The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.

- Information System – A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, whether automated or manual.

- Integrity – Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

- National Rules of Behavior – A set of Agency wide rules that describes the responsibilities and expected behavior of personnel with regard to information and information system usage.

- Privileged Users - individuals who have access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, system and network administrators, maintainers, system programmers).

- Risk – The level of impact on Agency operations (including mission, functions, image, or reputation), Agency assets, individuals, other organizations, or the Nation resulting from the operations of an information system given the potential impact of a threat and the likelihood of that threat occurring.

- Security Incident – An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

- Service – Activities and/or functions performed by a person, software, or hardware to satisfy requirements within the information system's environment.

- Service Manager – Person or organization having the responsibility for obtaining information technology services, e.g., cloud services. Services may be obtained as an enterprise solution or for a particular information owner's requirement. For enterprise solutions, service managers coordinate with the service providers to ensure information security requirements are met. For particular information owner solutions, service managers work with information owners to find appropriate service providers but the information owners ensure information security requirements are met. Service managers do not own the systems or the information.

- Signature (of an individual) – a mark or sign made by an individual to signify knowledge, approval, acceptance, or obligation. Can be accomplished manually, sometimes referred to as a "wet signature," or electronically.

- System Owner – Person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and final disposition of an information system.

- Written – or "in writing" means to officially document the action or decision and includes a signature. The documentation can be accomplished manually or electronically

## 9. 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 CISO and Director, OITO shall coordinate to maintain central repository of all waivers.

## 10. MATERIAL SUPERSEDED

*Information Security – Roles and Responsibilities Procedures*, CIO 2150.3-19.1.

## 11. CONTACTS

For further information, questions, or comments about this policy, please contact the OMS-EI, Office of Information Security and Privacy.

VAUGHN NOGA

Digitally signed by VAUGHN NOGA
Date: 2022.05.19 10:17:33 -04'00'

***Vaughn Noga***
***Deputy Assistant Administrator for Environmental Information and Chief Information Officer***
***U.S. Environmental Protection Agency***

## APPENDIX A: LIST OF ABBREVIATIONS

| | |
|---|---|
| AA | Assistant Administrator |
| AO | Authorizing Official |
| AODR | Authorizing Official Designated Representative |
| C&A | Certification and Accreditation |
| CCP | Common Criteria Provider |
| CIO | Chief Information Officer |
| CO | Contracting Officer |
| COR | Contracting Officer's Representative |
| CSIRC | Computer Security Incident Response Capability |
| DHS | Department of Homeland Security |
| FedRAMP | Federal Risk and Authorization Management Program |
| FIPS | Federal Information Processing Standard |
| FISMA | Federal Information Security Management Act |
| IG | Inspector General |
| IMO | Information Management Officer |
| IO | Information Owner |
| ISO | Information Security Officer |
| ISSO | Information System Security Officer |
| NIST | National Institute of Standards and Technology |
| NROB | National Rules of Behavior |
| NSOC | Network Security Operations Center |
| OARM | Office of Administration and Resource Management |
| OHS | Office of Homeland Security |
| OMB | Office of Management and Budget |
| OITO | Office of Information Technology Operations |
| PIA | Privacy Impact Assessment |
| PO | Privacy Officer |
| RA | Regional Administrator |
| RIF | Reduction In Force |
| CISO | Chief Information Security Officer |
| SAR | Security Assessment Report |
| SCA | Security Control Assessor |
| SIO | Senior Information Official |
| SM | Service Manager |
| SO | System Owner |
| SRO | Senior Resource Official |
| US-CERT | United States Computer Emergency Response Team |