EPA Classification No.: CIO 2150.3	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

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

ENVIRONMENTAL PROTECTION AGENCY INFORMATION SECURITY POLICY

1. PURPOSE

This policy establishes a program to provide security for Environmental Protection Agency (EPA) information and information systems, provides overarching direction for information security requirements, and defines responsibilities of the Administrator, Assistant Administrators (AAs), Regional Administrators (RAs), the Chief Information Officer (CIO), the Senior Agency Information Security Officer (SAISO), Senior Information Officials (SIOs), and other key officials. It is the formal, foundational policy from which all procedures, standards, guidelines and other EPA directives will be developed in defining and implementing information security requirements for EPA.

2. SCOPE AND APPLICABILITY

This policy covers all EPA information and information systems to include information and information systems used, managed, or operated by a contractor, another agency, or other organization on behalf of the agency.

This policy applies 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

This policy applies 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

The E-Government Act of 2002, Title III, *Federal Information Security Management Act* (FISMA) is the authority that governs how U.S. federal government agencies protect information resources. Additionally, agencies such as EPA, must comply with a host of other laws, regulations, policies, and guidelines that further outline requirements for how those resources must be protected, with the ultimate objectives of ensuring information confidentiality, integrity, and availability.

In response to FISMA, and other directives, EPA developed the *EPA Information Security Policy*. This policy establishes the EPA Information Security Program ensuring the protection of information and information systems that support EPA mission objectives. It does so by establishing a management structure, providing program direction, and identifying roles and responsibilities.

5. AUTHORITY

E-Government Act of 2002, Public Law 107-347, Title III, *Federal Information Security Management Act* (FISMA) as amended

Clinger-Cohen Act of 1996, Public Law 104-106

Privacy Act of 1974, Public Law 93-579, as amended

Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources,* November 28, 2000, *as revised*

OMB Memorandum M-11-29, *Chief Information Officer Authorities*, August 8, 2011

EPA Delegations of Authority, General, Administrative, and Miscellaneous: 1-19: *Directives*

EPA Delegations of Authority, General, Administrative, and Miscellaneous: 1-84: *Information Resources Management*

6. POLICY

The security of EPA information and information systems is vital to the success of EPA's mission. To that end, this policy establishes the EPA Information Security Program, a comprehensive agency-wide information security program that defines requirements, provides direction, and identifies, develops, implements, and maintains cost-effective solutions to protect EPA information, in any form or format, and supporting information systems used, managed, or operated by a contractor, another agency, or other organization. The National Institute of Standards and Technology information security related publications will be a primary reference used to implement policy requirements and the basis for EPA procedures, standards, guidance and other directives developed to support this policy. The EPA Information Security Program shall operate at all levels of the agency and include the following elements:

a) Periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency.

b) Policies and procedures that (a) are risk based, (b) cost-effectively reduce security risks to an acceptable level, (c) ensure that information security is addressed throughout the life cycle of each information system, and (d) ensure compliance with information security directives.

c) Definition and effective implementation of minimum, mandatory technical, operational, and management security controls, or other compensating countermeasures.

d) Subordinate plans for providing adequate security for all networks, facilities, and individual or groups of information systems that contain, process, store, or transmit EPA information.

e) Security awareness training for all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of EPA.

f) Role based information security training necessary for personnel, designated as having significant information security responsibilities, to carry out their information security responsibilities.

g) Periodic testing and evaluation of the effectiveness of management, operational, and technical controls of every system in the inventory. Frequency of testing and evaluation shall be based on risk, but not less than annually.

h) A process for planning, developing, implementing, evaluating, and documenting remedial actions to address deficiencies in information security controls.

i) Capabilities for detecting, reporting, and responding to security incidents where (a) risks are mitigated before substantial damage is done, (b) the central federal incident response center is notified and consulted, and (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.

j) Plans and procedures to ensure continuity of operations for agency systems.

k) EPA shall comply with the provisions of FISMA and related Office of Management and Budget (OMB) directives, National Institute of Standards and Technology (NIST) publications as required by FISMA and directed by OMB, and other higher level directives. EPA shall promulgate procedures, standards, guidelines and other directives as necessary under this policy to supplement, clarify and implement FISMA, OMB directives, NIST publications and other higher level directives.

l) EPA shall coordinate and cooperate with the Department of Homeland Security (DHS) as it carries out its federal government-wide information security responsibilities and activities.

7. ROLES AND RESPONSIBILITIES

The following roles are the core of the program; additional roles are identified and defined in supporting procedures as needed. Similarly with roles, additional and more prescriptive responsibilities are delineated in supporting procedures.

Re-delegation of assigned responsibilities shall be documented.

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

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

ii) Providing 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.

iii) Ensuring that information security management processes are integrated with agency strategic and operational planning processes.

iv) Ensuring that AAs and RAs and other key officials provide information security for the information and information systems that support the operations and assets under their control.

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

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

vii) Ensuring EPA has trained personnel sufficient to assist in complying with FISMA and other related information security directives.

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

ix) Ensuring annual Inspector General 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:

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

ii) Developing, documenting, implementing, and maintaining an agency-wide information security program as required by this policy, FISMA and related information security directives to enable and ensure EPA meets federal information security requirements.

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

iii) 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.

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

v) Assisting senior agency and other key officials with understanding and implementing their information security responsibilities.

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

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

viii) 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.

ix) Ensuring EPA SIOs and Information Security Officers (ISO) 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.

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

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

xii) Designating a Senior Agency Information Security Officer (SAISO) whose primary duty is information security in carrying out the CIO responsibilities under this policy and relevant information security laws, Executive Branch policy, and other directives.

xiii) Ensuring 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 this policy and relevant information security laws, Executive Branch policy, and other directives.

xiv) Ensuring the SAISO heads an office with the mission and resources required to administer the EPA Information Security Program functions, carry out the CIO responsibilities under this policy, and to assist in ensuring agency compliance with this policy.

xv) 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.

c) The **Senior Agency Information Security Officer (SAISO)** is responsible for:

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

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

d) **Assistant Administrators, Regional Administrators and Other Key Officials (e.g., Principal Deputy Assistant Administrators, Deputy Assistant Administrators, Deputy Region Administrators, Assistant Regional Administrators, Office Directors)** are responsible for:

i) Implementing the policies, procedures, control techniques, and other countermeasures promulgated under the EPA Information Security Program.

ii) Complying with FISMA and other related information security laws and requirements in accordance with the CIO directives to execute the appropriate security controls commensurate to responding to an EPA Network Security Operations Center (NSOC) security notification. Such CIO directives shall supersede and take priority over all operational tasks and assignments, and shall be complied with immediately.

iii) Ensuring that all employees within their organizations take immediate action to comply with directives from the CIO to (a) mitigate the impact of any potential information security risk, (b) respond to an information security incident, or (c) implement the provisions of a NSOC notification. Ensuring their organizational managers have all necessary authority and means to direct full compliance with such directives from the CIO.

iv) Enforcing and ensuring the EPA National Rules of Behavior, and additional rules of behavior for particular systems if established, is signed or acknowledged electronically or manually annually by all information and information system users that support the operations and assets of EPA.

e) A **Senior Information Official (SIO)** is responsible for:

i) 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.

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

iii) Designating, as needed, an Authorizing Official Designated Representative (AODR) to assist with AO duties.

(1) Designating and delegating responsibilities and authorities to the AODR in writing if not done so in existing policy.

(2) The authorization and associated risk acceptance decisions and signing the authorization to operate document cannot be delegated.

f) An **Authorizing Official Designated Representative (AODR)** is responsible for:

i) Carrying out the Authorizing Official's duties as assigned.

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

g) A **System Owner (SO)** is responsible for:

i) Coordinating with the CIO, SAISO, information owners, other system owners, and service managers regarding EPA Information Security Program requirements for the assigned system during its entire lifecycle.

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

iii) Coordinating with information owners for deciding 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 the assigned system.

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

v) Coordinating with the CIO, SAISO, 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 common and hybrid controls.

vi) Obtaining authorization to operate or test from the appropriate SIO prior to operational use or testing of any system.

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

h) An **Information Owner (IO)** is responsible for:

i) Providing assistance to the CIO, SAISO, 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.

ii) 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.

iii) Enforcing and ensuring the EPA National Rules of Behavior, 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.

iv) Determining and providing information to system owners 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, information owners will coordinate with system owners and service managers to establish and publish the additional rules of behavior.

v) Coordinating with the CIO, SAISO, systems owners, common control providers, and service mangers regarding information security requirements and determining and carrying out responsibilities for defining, developing, documenting, implementing, assessing, and monitoring common and hybrid controls.

i) An **Information Security Officer (ISO)** is responsible for:

i) 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.

ii) 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.

iii) Supporting system 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, monitored, and maintained to adequately protect supported information within acceptable risks.

iv) Coordinating with system owners, service managers and information owners in determining information security requirements, appropriate controls, and user access.

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

j) An **Information System Security Officer (ISSO)** is responsible for:

i) Supporting the SIO, SO, SM 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.

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

k) A **Common Control Provider** is responsible for:

i) Defining, developing, documenting, implementing, assessing, and monitoring common and hybrid controls provided.

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

iii) Providing approved security plans, security assessment reports, plans of action and milestones, and other information as necessary under the EPA Information Security Program for provided common controls to supported system owners, information owners, and service managers inheriting those controls.

l) The **Inspector General** is responsible for:

i) Conducting an annual audit of the EPA information security program.

ii) Reporting annually audit results to the EPA Administrator.

m) **EPA information and information system Users,** i.e., employees, contractors, grantees, and others, that support the operations and assets of EPA are responsible for:

i) Complying with all agency information security policies, procedures, and other directives.

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

iii) Reporting all suspected and actual information security incidents immediately.

iv) Annually signing or acknowledging electronically or manually that they have read, understand, and agree to abide by the EPA National Rules of Behavior, and any additional rules of behavior for particular systems if established.

8. RELATED DOCUMENTS

OMB M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security*, July 6, 2010

9. 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.

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 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.

Subordinate Plan – Also referred to as a system security plan, is a formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.

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.

10. WAIVERS

N/A

11. RELATED POLICY, PROCEDURES, STANDARDS AND GUIDELINES

Related policy, procedures, standards and guidelines are available on OEI's Policy Resources website.

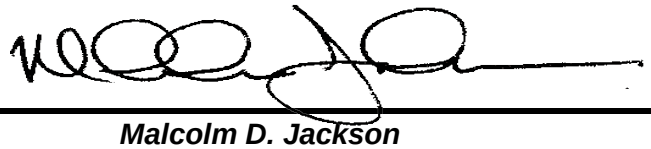
12. MATERIAL SUPERSEDED

CIO 2150.2 Interim Agency Information Security Policy

2195A1 EPA Information Security Manual, 1999 Edition

13. ADDITIONAL INFORMATION

For further information, questions, or comments about this policy, please contact the Office of the EPA Senior Agency Information Security Officer.



Malcolm D. Jackson
Assistant Administrator and Chief Information Officer
Office of Environmental Information

APPENDIX A: ACRONYMS

AA	Assistant Administrator
AO	Authorizing Official
AODR	Authorizing Official Designated Representative
ARA	Assistant Regional Administrator
CIO	Chief Information Officer
SAISO	Senior Agency Information Security Officer
EPA	Environmental Protection Agency
FISMA	Federal Information Security Management Act
IO	Information Owner
ISO	Information Security Officer
ISSO	Information System Security Officer
NSOC	Network Security Operations Center
OEI	Office of Environmental Information
OMB	Office of Management and Budget
RA	Regional Administrator
SIO	Senior Information Official
SM	Service Manager
SO	System Owner