INFORMATION DIRECTIVE
POLICY

Information Security Policy		
Directive No.: CIO 2150.5	CIO Approval: August 2019	Review Date: August 2021

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

Information Security Policy

1. PURPOSE

The Information Security 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 (AA), Regional Administrators (RA), the Chief Information Officer (CIO), the Chief Information Security Office (CISO), Senior Information Officials (SIO) and other key officials. The policy is the formal, foundational documentation from which all procedures, standards, guidance and other EPA directives will be developed in defining and implementing information security requirements for EPA.

2. SCOPE

The 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.

3. AUDIENCE

The policy applies to all EPA employees, contractors, grantees and all other users of EPA information and information systems supporting the operations and assets of EPA.

4. BACKGROUND

The *Federal Information Security Modernization Act of 2014* (FISMA) is the authority governing 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 further outlining 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*. The policy establishes the EPA Information Security Program, which ensures the protection of information and information systems supporting EPA mission objectives by establishing a management structure, providing program direction, and identifying roles and responsibilities.

5. AUTHORITY

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

Additional legal foundations for the procedure include:

- E-Government Act of 2002, Public Law 107-347, Title III, Federal Information Security Management Act, as amended
- Federal Information Security Modernization Act of 2014, Public Law 113-283, chapter 35 of title 44, United States Code (U.S.C.)
- Clinger-Cohen Act of 1996, Public Law 104-106
- Privacy Act of 1974 (5 U.S.C. § 552a), as amended
- Office of Management and Budget (OMB) Circular A-130, “Managing Information as a Strategic Resource,” as revised
- 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 adequate, risk-based, cost-effective solutions to protect all EPA information created, collected, processed, stored, transmitted, disseminated, or disposed of by or on behalf of the agency, to include EPA information residing in contractor, another agency, or other organization information systems and networks, in any form or format. The National Institute of Standards and Technology (NIST) information security related publications are the primary references 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:

- 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 supporting the operations and assets of the agency. Steps are taken to maintain risk at an acceptable level within the agency’s risk tolerance across the three organizational tiers, the enterprise level, the mission or business process level, and the information and information system level.

- Policies and procedures that: (a) are risk-based; (b) cost-effectively reduce security risks to comply with the information system security categorization level; (c) ensure that information security is addressed throughout the life cycle of each information system and (d) ensure compliance with information security directives.
- Systems security engineering principles, concepts, and techniques are employed during the life cycle of information systems to facilitate the development, deployment, operation, and sustainment of trustworthy and adequately secure systems.
- Supply chain risk management principles are employed to protect against the insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software, as well as poor manufacturing and development practices throughout the system development life cycle.
- Definition and effective implementation of minimum mandatory technical, operational and management security controls or other compensating countermeasures.
- 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.
- Mandatory security awareness training for all EPA employees, contractors and all other users of EPA information and information systems supporting the operations and assets of EPA.
- Mandatory role-based information security training for personnel designated as having significant information security responsibilities to carry out their information security responsibilities.
- Periodic testing and evaluation of management, operational and technical controls for every system in the inventory to ensure controls are working as intended. Frequency of testing and evaluation shall be based on risk.
- Continuous monitoring of controls in accordance with the agency's Information Security Continuous Monitoring Strategic Plan.
- A process for planning, developing, implementing, evaluating and documenting remedial actions to address deficiencies in information security controls.
- Capabilities for detecting, reporting, and responding to security incidents where
    - risks are mitigated before substantial damage is done;
    - the central federal incident response center is notified and consulted; and
    - law enforcement agencies and the EPA Office of Inspector General (IG) and any other agency or office in accordance with law or as directed by the President are notified and consulted as appropriate.
- Plans and procedures to ensure continuity of operations for agency systems and so that security controls remain effective over time.

EPA shall comply with the provisions of FISMA, OMB A-130 and other related OMB directives, NIST publications as required by FISMA and directed by OMB, and Department of Homeland Security (DHS), Office of Personnel Managment (OPM) and other higher-level directives. EPA shall promulgate procedures, standards, guidance and other directives as necessary under this policy to supplement, clarify and implement FISMA, OMB directives, NIST publications, and DHS, OPM and other higher-level directives.

EPA shall coordinate and cooperate with the 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. As with roles, additional and more prescriptive responsibilities are delineated in supporting procedures.

Re-delegation of assigned responsibilities shall be documented.

EPA Administrator

1) The EPA Administrator is responsible for:
   a) Ensuring that an agency-wide information security program is developed, documented, implemented and maintained to protect information and information systems.
   b) Providing information security protections that are commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification or destruction of information collected or maintained by or on behalf of the agency and on information systems used, managed or operated by the agency, another agency or by a contractor or other organization on behalf of the agency.
   c) Ensuring that information security management processes are integrated with agency strategic and operational planning processes.
   d) Ensuring that AAs, RAs and other key officials provide information security for the information and information systems that support the operations and assets under their control.
   e) Ensuring enforcement and compliance with FISMA and related information security directives.
   f) Delegating to the CIO the authority to ensure compliance with FISMA and related information security directives.
   g) Ensuring EPA has trained personnel to sufficiently assist in complying with FISMA and other related information security directives.
   h) Ensuring that the CIO, in coordination with AAs, 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.

- i) Ensuring annual IG information security audit results are reported to Congress, OMB, DHS and other entities as required by law and Executive Branch direction.

Chief Information Officer (CIO)

1) The CIO is responsible for:
    - a) Ensuring the EPA Information Security Program and protection measures are compliant with FISMA and related information security directives.
    - b) 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.
        - i) Developing, documenting, implementing and maintaining agency-wide, well designed, well managed continuous monitoring and standardized risk assessment processes.
    - c) Developing, maintaining and issuing agency-wide information security policies, procedures and control techniques to provide direction for implementing the requirements of the EPA Information Security Program.
    - d) Training and overseeing personnel with significant information security responsibilities with respect to such responsibilities.
    - e) Assisting senior agency and other key officials with understanding and implementing their information security responsibilities.
    - f) Establishing minimum mandatory risk-based technical, operational and management information security control requirements for agency information and information systems.
    - g) Reporting any compliance failure or policy violation directly to the appropriate AA, RA or other key officials for appropriate disciplinary and corrective action.
    - h) Requiring any AA, RA or other key official so notified to report to the CIO regarding what actions are to be taken in response to any compliance failure or policy violation reported by the CIO.
    - i) 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.
    - j) Establishing the EPA National Rules of Behavior (NROB) for appropriate use and protection of the information and information systems supporting the EPA mission and functions.
    - k) Developing, implementing and maintaining capabilities for detecting, reporting and responding to information security incidents.
    - l) Designating a CISO whose primary duty is information security to carry out the CIO responsibilities under this policy and relevant information security laws, Executive Branch policy and other directives.

  - m) Ensuring 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 this policy and relevant information security laws, Executive Branch policy and other directives.
  - n) Ensuring 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 this policy and assist in ensuring agency compliance with this policy.
  - o) 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.

Chief Information Security Officer (CISO)

1) The CISO is responsible for:
  - a) Carrying out the CIO responsibilities under this policy and relevant information security laws, Executive Branch policy and other directives.
  - b) 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.

Assistant Administrators (AA), Regional Administrators (RA) and Other Key Officials

1) AAs, RAs and other key officials (e.g., Principal Deputy Assistant Administrators, Deputy Assistant Administrators, Deputy Regional Administrators, Mission Support Division Directors and Office Directors) are responsible for:
  - a) Implementing the policies, procedures, control techniques and other countermeasures promulgated under the EPA Information Security Program.
  - b) Complying with FISMA and other related information security laws and requirements in accordance with CIO directives to execute the appropriate security controls commensurate with responding to an EPA Security Operations Center (SOC) security notification. Such CIO directives shall supersede and take priority over all operational tasks and assignments, and shall be complied with immediately.
  - c) 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 SOC notification.
  - d) Ensuring their organizational managers have all necessary authority and means to direct full compliance with directives from the CIO.
  - e) Enforcing and ensuring the EPA NROB and additional rules of behavior for particular systems, if established, are annually signed or acknowledged electronically or manually by all information users and information system users that support the operations and assets of EPA.

Senior Information Officials (SIO)

1) SIOs are responsible for:
    a) Ensuring effective processes, procedures and other directives are established as needed 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 to maintain risk within the agency’s acceptable thresholds at the mission or business process level and the information and information system level.
    b) Carrying out the duties of the Authorizing Official (AO) for their office or region.
    c) Designating an Authorizing Official Designated Representative (AODR) as needed to assist with AO duties.
        i) Designate and delegate responsibilities and authorities to the AODR in writing as needed to supplement existing policies.
    d) Accepting risk, authorization decisions and signing or acknowledging electronically or manually an authorization to operate (ATO).
        i) Conducting reauthorizations follow agency ongoing authorization procedures and processes.

Authorizing Official Designated Representatives (AODR)

1) AODRs are responsible for:
    a) Carrying out AO duties that do not include accepting risk to organizational operations and assets, individuals, other organizations and the Nation or in any manner acknowledging or signing an ATO.
    b) 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.

Information Security Officers (ISO)

1) ISOs are responsible for:
    a) 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.
    b) Supporting the SIO in ensuring effective processes and procedures and other directives are established as necessary to implement and enforce the policies, procedures, control techniques and other countermeasures identified under the EPA Information Security Program for their office or region.
    c) Supporting System Owners (SO) and Service Managers (SM) 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 the agency’s acceptable risk thresholds.
    d) Coordinating with SOs, SMs, and Information Owners (IO) to determine information security requirements, appropriate controls and user access.

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

System Owners (SO)

1) SOs are responsible for:
   a) Coordinating with the CIO, CISO, IOs, other SOs and SMs regarding EPA Information Security Program requirements for the assigned system during its entire lifecycle.
   b) Developing, maintaining and providing information security documents as required under the EPA Information Security Program for the assigned system.
   c) Coordinating with IOs to decide 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.
   d) Coordinating with IOs and SMs to determine if additional rules of behavior are needed for particular systems beyond those provided in the NROB. If additional rules of behavior are needed, SOs will coordinate with IOs and SMs to establish and publish the additional rules of behavior.
   e) Coordinating with the CIO, CISO, Common Control Providers (CCP), IOs and SMs regarding information security requirements and determining and carrying out responsibilities for defining, developing, documenting, implementing, assessing and monitoring common and hybrid controls.
   f) Obtaining authorization to operate or test from the appropriate SIO prior to operational use or testing of any system.
   g) Configuring, continuously monitoring and maintaining systems to adequately protect information stored, processed or transmitted within acceptable risks.

Information Owners (IO)

1) IOs are responsible for:
   a) Assisting the CIO, CISO, SOs, CCPs and SMs 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.
   b) Approving user access to a system or service, to include types of privileges and access rights, that contains information for which the IO is responsible.
   c) Enforcing and ensuring the EPA NROB and additional rules of behavior for particular systems, if established, are annually signed or acknowledged electronically by all information users that support the operations and assets of EPA for information for which the IO is responsible.
   d) Determining and providing information to SOs and SMs on additional rules of behavior needed beyond those provided in the NROB for particular systems. If additional rules of behavior are needed, IOs will coordinate with SOs and SMs to establish and publish the additional rules of behavior.
   e) Coordinating with the CIO, CISO, SOs, CCPs and SMs regarding information security requirements, and determining and carrying out responsibilities for

defining, developing, documenting, implementing, assessing and monitoring common and hybrid controls.

Information System Security Officers (ISSO)

1) ISSOs are responsible for:
    a) Supporting the SIO, SO, SM and ISO to manage and implement 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.
    b) Serving as a principal advisor on all matters, technical and otherwise, involving the security of the information, information system or service assigned.

Common Control Providers (CCP)

1) CCPs are responsible for:
    a) Defining, developing, documenting, implementing, assessing and monitoring common and hybrid controls provided.
    b) Coordinating with the CIO, SOs, IOs and SMs regarding information security requirements and determining and carrying out responsibilities for defining, developing, documenting, implementing, assessing and monitoring common and hybrid controls.
    c) 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 SOs, IOs and SMs inheriting those controls.

Inspector General (IG)

1) The IG is responsible for:
    a) Conducting an annual audit of the EPA Information Security Program.
    b) Reporting annual audit results to the EPA Administrator.

Users

1) EPA information and information system Users (i.e., employees, contractors, grantees, and others) supporting or using the operations and assets of EPA are responsible for:
    a) Complying with all agency information security policies, procedures and other directives.
    b) Successfully completing information security awareness training prior to initial access to EPA systems and at least annually thereafter to maintain access.
    c) Reporting all suspected and actual information security incidents immediately.
    d) Signing or acknowledging electronically or manually they have read, understand and agree to abide by the EPA NROB and any additional system-specific rules of behavior if established prior to their initial access to EPA systems and information and at least annually thereafter to maintain access.

e) In addition, users designated as having significant information security responsibilities are responsible for:
   a) Successfully completing information security role-based training prior to initial access to EPA systems in their designated role(s) and at least annually thereafter to maintain access.

8. RELATED INFORMATION

- OMB M-10-28, “Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS),” July 6, 2010
- OMB M-16-15, “Federal Cybersecurity Workforce Strategy,” July 12, 2016 OMB Circular A-123, “Management’s Responsibility for Internal Controls”

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.
- **Authorization package:** The essential information that an authorizing official uses to determine whether to authorize the operation of an information system or the use of a designated set of common controls. At a minimum, the authorization package includes the information system security plan, privacy plan, security control assessment, privacy control assessment, and any relevant plans of action and milestones.
- **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.
- **Federal information:** Information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.
- **Federal information system:** An information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency.

- **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 security continuous monitoring:** Maintaining ongoing awareness of information security, vulnerabilities, threats, and incidents to support agency risk management decisions[1].
- **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.
- **Ongoing authorization:** The risk determinations and risk acceptance decisions subsequent to the initial authorization, taken at agreed-upon and documented frequencies in accordance with the agency's mission or business requirements and agency risk tolerance. Ongoing authorization is a time-driven or event-driven authorization process whereby the authorizing official is provided with the necessary and sufficient information regarding the security and privacy state of the information system to determine whether the mission or business risk of continued system operation is acceptable.
- **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

---

[1] *The terms continuous and ongoing in this context mean that security controls and agency risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect agency information.*

as an enterprise solution or for a particular IO's requirement. For enterprise solutions, SMs coordinate with the service providers to ensure information security requirements are met. For particular IO solutions, SMs work with IOs to find appropriate service providers but the IOs ensure information security requirements are met. SMs 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):** to officially document the action or decision, either manually or electronically, and includes a signature.

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

10. WAIVERS

N/A

11. MATERIAL SUPERSEDED

- CIO 2150.3 Environmental Protection Agency Information Security Policy
- 2195A1 EPA Information Security Manual, 1999 Edition

12. CONTACTS

For further information, questions, or comments about this policy, please contact the Office of Mission Support (OMS), Office of Information Security & Privacy (OISP).

VAUGHN NOGA

Digitally signed by VAUGHN NOGA
Date: 2019.08.27 16:52:58 -04'00'

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

Information Security Policy		
Directive No.: CIO 2150.5	CIO Approval: August 2019	Review Date: August 2021

APPENDIX
ACRONYMS & ABBREVIATIONS

AA	Assistant Administrator
AO	Authorizing Official
AODR	Authorizing Official Designated Representative
ATO	Authorization to Operate
CCP	Common Control Provider
CIO	Chief Information Officer
DHS	Department of Homeland Security
EPA	Environmental Protection Agency
FISMA	Federal Information Security Modernization Act
IG	Inspector General
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
OMS	Office of Mission Support
OISP	Office of Information Security & Privacy
OMB	Office of Management and Budget
RA	Regional Administrator
CISO	Chief Information Security Officer
SIO	Senior Information Official
SM	Service Manager
SO	System Owner