Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19

Information Security Policy

1. PURPOSE

As Information systems and networks have increased in complexity, safeguarding Federal government operations, financial resources, property, and information has become more challenging. Moreover, sensitive information and non-public information, including private information about individuals (for example, personal identifiable information (PII) about Environmental Protection Agency (EPA) or contractor personnel and members of the general public, including Social Security Numbers) or confidential business information is vulnerable to inappropriate use, accidental disclosure, or malicious compromise. The systems and information covered by this policy require ongoing assessments and management oversight to ensure comprehensive protection. To be effective, a comprehensive, integrated “defense in depth” approach to managing Information Technology (IT) resources is required that incorporates security and business objectives.

The EPA must ensure that all information systems are protected from threats to confidentiality, integrity, and availability to a degree commensurate with the potential impact from a compromise. The EPA maintains a variety of information systems that support the Agency's mission. EPA information systems depend on adequate information, personnel, and physical security for proper operation and protection from unauthorized access and modification. The increased number and complexity of network attacks and the inherent vulnerability of networked information systems require a rigorous approach to protect the integrity of EPA information systems.

The Information Security Policy establishes minimum standards for information security requirements and assigns organizational and management responsibility to ensure the implementation of Federal security mandates including, but not limited to, the Federal Information Security Modernization Act (FISMA) of 2014, Office of Management and Budget (OMB) Circular No. A-130, other statutes and regulations (see Authorities Section 4) and Agency directives and guidance such as the EPA Cybersecurity Handbook for EPA information and information systems. 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 United States 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 EPA.

3. AUDIENCE

Senior Information Officials (SIO), Information Security Officers (ISO), Liaison Privacy Officials (LPO) and EPA System Owners (SO) or their official designees, for EPA-

operated systems, and Service Managers (SM), for systems operated on behalf of the EPA, EPA employees, contractors and all other users of EPA information and systems.

4. AUTHORITY

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

- E-Government Act of 2002, Public Law 107-347, Title III, Federal Information Security Management Act, as amended
- Clinger-Cohen Act of 1996, Public Law 104-106
- Privacy Act of 1974 (5 U.S.C. § 552a), as amended
- Federal Information Security Modernization Act (FISMA) of 2014, Public Law 113-283, to amend chapter 35 of title 44, United States Code (U.S.C.)
- Office of Management and Budget (OMB) Circular A-130, "Managing Information as a Strategic Resource," July 2016
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations, September 2020
- NIST SP 800-53B, Control Baselines for Information Systems and Organizations, October 2020
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004
- 32 CFR 2002 - CONTROLLED UNCLASSIFIED INFORMATION (CUI)

5. POLICY

The security of EPA information and information systems is vital to the success of the EPA's mission. To that end, this policy establishes the minimum requirements for the EPA Information Security Program (ISP). The ISP is 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 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.

Under the guidance of the CIO and the Chief Information Security Officer (CISO), EPA Regional and Program Office IT and IT Security stakeholders; including but not limited to, SIO, Information Management Officials (IMO), Information Resource Manager Branch Chiefs (IRMBC), SO and ISO, will ensure full compliance with this policy and supporting procedures and guidelines.

The EPA ISP shall operate at all levels of the agency and include the following elements:

- Defined roles and responsibilities associated with implementing and complying with the EPA ISP.
- A framework for implementing continuous improvement to stay ahead of cyber threats while aligning with and facilitating dynamic changes in mission and business requirements.
- A comprehensive risk management strategy which will include 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.
- Agency-level policies and procedures that: (a) are risk-based; (b) cost-effectively reduce risks through compliance with the information security directives; and (c) ensure that information security is addressed throughout the life cycle of each information system.
- 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.
- Plans and procedures to ensure continuity of minimum mandatory technical, operational and management security controls or other compensating countermeasures.
- Definition and effective implementation of minimum mandatory technical, operational and management security controls or other compensating countermeasures.
- Comprehensive inventory of all EPA information systems including subordinate plans identifying the security controls implemented for each system.
- Information Security Continuous Monitoring Strategy (ISCMS) which includes ongoing security assessments and periodic testing and evaluation of management, operational and technical controls.
- A process for planning, developing, implementing, evaluating and documenting remedial actions to address deficiencies in information security controls.
- Develop workforce management procedures, services, and capabilities in support of a well-trained and qualified cybersecurity workforce through a comprehensive security and privacy education and awareness and training program, including role-based training program for users with significant security responsibilities.
- 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;
    - 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; and
    - cybersecurity and threat information are incorporated and shared as

needed to support EPA and the Nation's cybersecurity objectives.

6. ROLES AND RESPONSIBILITIES

The Information Security – Roles and Responsibilities procedure 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.

7. 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 Enterprise Risk Management and Internal Control," July 2016
- EPA Roles and Responsibilities Procedures
- EPA Delegations of Authority, General, Administrative, and Miscellaneous: 1-19: "Directives"
- EPA Delegations of Authority, General, Administrative, and Miscellaneous: 1-84: "Information Resources Management"

8. DEFINITIONS

- **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, 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 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]

[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.*

- **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.
- **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.
- **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.
- **Written (or in writing)** – to officially document the action or decision, either manually or electronically, and includes a signature.

9. WAIVERS

The full compliance with this policy is mandatory and waivers will not be accepted.

10. DIRECTIVE(S) SUPERSEDED

This procedure supersedes Information Directive: CIO 2150.5 Information Security Policy and 2195A1 EPA Information Security Manual, 1999 Edition.

11. CONTACTS

For further information about this directive, please contact the Office of Mission Support (OMS), Office of Information Security and Privacy (OISP) at Infosec@epa.gov.

VAUGHN NOGA

Digitally signed by VAUGHN NOGA
Date: 2024.02.01 09:00:37 -05'00'

Vaughn Noga, Chief Information Officer and Deputy Assistant Administrator for Information Technology and Information Management

APPENDIX A: 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