EPA IT/IM DIRECTIVE
PROCEDURE

Information Security – Program Management (PM) Procedure

Directive No: CIO 2150-P-23.2

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

Information Security – Program Management (PM) Procedure

1. PURPOSE

The Environmental Protection Agency (EPA) is responsible for ensuring all offices within the Agency meet the minimum-security requirements defined in the Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. All EPA information systems shall meet the security requirements by implementing the security controls defined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.

The purpose of this procedure is to facilitate the implementation of the EPA security control requirements for the Program Management (PM) control family, as identified in NIST SP 800-53, Revision 5.

2. SCOPE

These procedures address 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 EPA.

3. AUDIENCE

Senior Information Officials (SIO), Information Security Officers (ISO) 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

- 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
- 32 CFR 2002 for Controlled Unclassified Information (CUI)

5. PROCEDURE

SIO, ISO and EPA SO or their official designees for EPA-operated systems; and SM, for systems operated on behalf of the EPA and to the extent made applicable to their management of the system through a contract or other appropriate mechanism, are responsible for implementing the controls in this procedure. EPA is adopting this procedure agency-wide, and expects these officials to develop a plan with timelines for adoption for their system(s). EPA employees, contractors and all other users of EPA information and information systems that support the operations and assets of the EPA should be aware of the content of this procedure and should follow the directions provided by SIO, ISO and EPA SO or their official designees and SM for the systems that they oversee.

The "PM" designator (e.g., PM-2, PM-3) identified for each procedure below corresponds to the NIST- identifier for the Program Management control family, as identified in NIST SP 800-53, Revision 5*.*

NIST defines the applicable Security and Privacy baseline controls in NIST 800-53B, *Control Baselines for Information Systems and Organizations.*
The PM controls are implemented at the organization level supporting the Agency's overall information security program and not directed at individual information systems.
The PM controls are independent of FIPS 200 impact levels and, therefore, are not associated with the individual systems control baselines. The controls included in the Privacy Control Baseline are identified below the control name.

PM-1 – Information Security Program Plan

1) Develop and disseminate an organization-wide information security program plan that:
    a) Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
    b) Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
    c) Reflects the coordination among organizational entities responsible for information security; and
    d) Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;
2) Review and update the organization-wide information security program plan annually and following organizational changes, problems identified during plan implementation or as directed by management to meet new federal law, mandate, or Agency direction; and
3) Protect the information security program plan from unauthorized disclosure and modification.

PM-2 – Information Security Program Leadership Role

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

PM-3 – Information Security and Privacy Resources

For Privacy Control Baseline:

1) Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement;
2) Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards; and
3) Make available for expenditure, the planned information security and privacy resources.

PM-4 – Plan of Action and Milestones Process

For Privacy Control Baseline:

1) Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems:
   a) Are developed and maintained;
   b) Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and
   c) Are reported in accordance with established reporting requirements.
2) Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

PM-5 – System Inventory

1) Develop and update annually an inventory of organizational systems.

PM-5(1) – System Inventory | Inventory of Personally Identifiable Information

For Privacy Control Baseline:

1) Establish, maintain, and update annually, when a system begins to collect PII, or when the types of PII being processed changes, an inventory of all systems, applications, and projects that process personally identifiable information.

PM-6 – Measures of Performance

For Privacy Control Baseline:

1) Develop, monitor and report on the results of information security and privacy measures of performance.

PM-7 – Enterprise Architecture

For Privacy Control Baseline:

1) Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.

PM-7(1) – Enterprise Architecture | Offloading

1) Offload non-essential functions or services, as feasible, to other systems, system components, or an external provider.

PM-8 – Critical Infrastructure Plan

For Privacy Control Baseline:

1) Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

PM-9 – Risk Management Strategy

For Privacy Control Baseline:

1) Develops a comprehensive strategy to manage:
   a) Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; and
   b) Privacy risk to individuals resulting from the authorized processing of personally identifiable information;
2) Implement the risk management strategy consistently across the organization; and
3) Review and update the risk management strategy annually or as required, to address organizational changes.

PM-10 – Authorization Process

For Privacy Control Baseline:

1) Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes;
2) Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and
3) Integrate the authorization processes into an organization-wide risk management program.

PM-11 – Mission and Business Process Definition

For Privacy Control Baseline:

1) Define organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations and the Nation; and
2) Determine information protection and personally identifiable information processing needs arising from the defined mission and business processes; and
3) Review and revise the mission and business processes annually or as the business/mission of the system changes.

PM-12 – Insider Threat Program

1) Implement an insider threat program that includes a cross-discipline insider threat incident handling team.

PM-13 – Security and Privacy Workforce

For Privacy Control Baseline:

1) Establish a security and privacy workforce development and improvement program.

PM-14 – Testing, Training, and Monitoring

For Privacy Control Baseline:

1) Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems:
   a) Are developed and maintained; and

   b) Continue to be executed; and
2) Review testing, training and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

<u>PM-15 – Security and Privacy Groups and Associations</u>

1) Establish and institutionalize contact with selected groups and associations within the security and privacy communities:
   a) To facilitate ongoing security and privacy education and training for organizational personnel;
   b) To maintain currency with recommended security and privacy practices, techniques, and technologies; and
   c) To share current security and privacy information, including threats, vulnerabilities, and incidents.

<u>PM-16 – Threat Awareness Program</u>

1) Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.

<u>PM-16(1) – Threat Awareness Program | Automated Means for Sharing Threat Intelligence</u>

1) Employ automated mechanisms to maximize the effectiveness of sharing threat intelligence information.

<u>PM-17 – Protecting Controlled Unclassified Information on External Systems</u>
For Privacy Control Baseline:

1) Establish policy and procedures to ensure that requirements for the protection of controlled unclassified information that is processed, stored or transmitted on external systems, are implemented in accordance with applicable laws, executive orders, directives, policies, regulations, and standards; and
2) Review and update the policy and procedures annually or as required by federal law, mandate, or Agency direction.

<u>PM-18 – Privacy Program Plan</u>
For Privacy Control Baseline:

1) Develop and disseminate an organization-wide privacy program plan that provides an overview of the agency’s privacy program, and:
   a) Includes a description of the structure of the privacy program and the resources dedicated to the privacy program;
   b) Provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements;
   c) Includes the role of the senior agency official for privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities;
   d) Describes management commitment, compliance, and the strategic goals and objectives of the privacy program;
   e) Reflects coordination among organizational entities responsible for the different aspects of privacy; and
   f) Is approved by a senior official with responsibility and accountability for the privacy risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other

organizations, and the Nation; and

2) Update the plan annually or as required by federal law, mandate, or Agency direction and to address changes in federal privacy laws and policy and organizational changes and problems identified during plan implementation or privacy control assessments.

PM-19 – Privacy Program Leadership Role

For Privacy Control Baseline:

1) Appoint a senior agency official for privacy with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the organization-wide privacy program.

PM-20 – Dissemination of Privacy Program Information

For Privacy Control Baseline:

1) Maintain a central resource webpage on the organization’s principal public website that serves as a central source of information about the organization’s privacy program and that:
   a) Ensures that the public has access to information about organizational privacy activities and can communicate with its senior agency official for privacy;
   b) Ensures that organizational privacy practices and reports are publicly available; and
   c) Employs publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.

PM-20(1) – Dissemination of Privacy Program Information | Privacy Policies on Websites, Applications, and Digital Services

For Privacy Control Baseline:

1) Develop and post privacy policies on all external-facing websites, mobile applications, and other digital services, that:
   a) Are written in plain language and organized in a way that is easy to understand and navigate;
   b) Provide information needed by the public to make an informed decision about whether and how to interact with the organization; and
   c) Are updated whenever the organization makes a substantive change to the practices it describes and includes a time/date stamp to inform the public of the date of the most recent changes.

PM-21 – Accounting of Disclosures

For Privacy Control Baseline:

1) Develop and maintain an accurate accounting of disclosures of personally identifiable information, including:
   a) Date, nature, and purpose of each disclosure; and
   b) Name and address, or other contact information of the individual or organization to which the disclosure was made;
2) Retain the accounting of disclosures for the length of the time the personally identifiable information is maintained or five years after the disclosure is made, whichever is longer; and
3) Make the accounting of disclosures available to the individual to whom the personally identifiable information relates upon request.

PM-22 – Personally Identifiable Information Quality Management

For Privacy Control Baseline:

1) Develop and document organization-wide policies and procedures for:
    a) Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle;
    b) Correcting or deleting inaccurate or outdated personally identifiable information;
    c) Disseminating notice of corrected or deleted personally identifiable information to individuals or other appropriate entities; and
    d) Appeals of adverse decisions on correction or deletion requests.

PM-23 – Data Governance Body

1) Establish a Data Governance Body consisting of CIO, CISO, Chief Data Officer (CDO), Office of General Counsel (OGC) representative, Regional/Program Office Representatives, and Controlled Unclassified Information (CUI) Program Office Director or above in accordance with Enterprise Data Management Policy (EDMP) and Agency Data Standards.

PM-24 – Data Integrity Board

For Privacy Control Baseline:

1) Establish a Data Integrity Board to:
    a) Review proposals to conduct or participate in a matching program; and
    b) Conduct an annual review of all matching programs in which the agency has participated.

PM-25 – Minimization of Personally Identifiable Information Used in Testing, Training, and Research

For Privacy Control Baseline:

1) Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research;
2) Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;
3) Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; and
4) Review and update policies and procedures annually or as the business/mission of the system changes.

PM-26 – Complaint Management

For Privacy Control Baseline:

1) Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and privacy practices that includes:
    a) Mechanisms that are easy to use and readily accessible by the public;
    b) All information necessary for successfully filing complaints;
    c) Tracking mechanisms to ensure all complaints received are reviewed and addressed within 30 business days;
    d) Acknowledgement of receipt of complaints, concerns, or questions from individuals within 3 to 5 business days; and
    e) Response to complaints, concerns, or questions from individuals within 15 business days.

PM-27 – Privacy Reporting

For Privacy Control Baseline:

1) Develop privacy reports as determined by federal legislation or the National Privacy Program (NPP) and disseminate to:
    a) The EPA Senior Agency Official for Privacy (SAOP), Chief Privacy Officer (CPO), Agency Privacy Officer (APO) and SIO to demonstrate accountability with statutory, regulatory, and policy privacy mandates; and
    b) Information Management Officials (IMO); Information Resource Management Branch Chiefs (IRMBC), Liaison Privacy Officers (LPO) and other personnel with responsibility for monitoring privacy program compliance; and
2) Review and update privacy reports annually or as directed by federal legislation or the NPP.

PM-28 – Risk Framing

For Privacy Control Baseline:

1) Identify and document:
    a) Assumptions affecting risk assessments, risk responses, and risk monitoring;
    b) Constraints affecting risk assessments, risk responses, and risk monitoring;
    c) Priorities and trade-offs considered by the organization for managing risk; and
    d) Organizational risk tolerance;
2) Distribute the results of risk framing activities to the EPA CPO, APO, SIO, SO, ISO, IMO, IRMBC, and LPO; and
3) Review and update risk framing considerations annually or as directed by federal legislation or the NPP.

PM-29 – Risk Management Program Leadership Roles

1) Appoint a Senior Accountable Official for Risk Management to align organizational information security and privacy management processes with strategic, operational, and budgetary planning processes; and
2) Establish a Risk Executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across the organization.

PM-30 – Supply Chain Risk Management Strategy

1) Develop an organization-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services;
    a) Implement the supply chain risk management strategy consistently across the organization; and
        i) Review and update the supply chain risk management strategy on annual basis or as required, to address organizational changes.

PM-30(1) – Supply Chain Risk Management Strategy | Suppliers of Critical or Mission-essential Items

1) Identify, prioritize, and assess suppliers of critical or mission-essential technologies, products, and services.

PM-31 – Continuous Monitoring Strategy

For Privacy Control Baseline:

1) Develop an organization-wide continuous monitoring strategy and implement

continuous monitoring programs that include:

a) Establishing the following organization-wide metrics to be monitored: as defined by the CISO or federal legislation, mandates, directives;
b) Establishing annually for monitoring and annually for assessment of control effectiveness;
c) Ongoing monitoring of organizationally-defined metrics in accordance with the continuous monitoring strategy;
d) Correlation and analysis of information generated by control assessments and monitoring;
e) Response actions to address results of the analysis of control assessment and monitoring information; and
f) Reporting the security and privacy status of organizational systems to the CISO monthly.

PM-32 – Purposing

Analyze all systems that directly support the Agency Primary Mission Essential Functions (PMEF) or Mission Essential Functions (MEF) supporting mission essential services or functions to ensure that the information resources are being used consistent with their intended purpose.

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

- The National Strategy to Secure Cyberspace, February 2003
- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures
- EPA CUI Policy
- EPA CUI Procedure

8. DEFINITIONS

- **Information Security** – the practice of defending information from unauthorized access, use, disclosure, disruption, modification or destruction, usually by enacting security controls.
- **Information Security Policy** – an aggregate of directives, regulations, rules and practices that prescribe how an organization manages, protects and distributes information.
- **Information System Management** – administering databases, network components, workstations or servers — typically requiring privileged users' access.

- **Plan of Action and Milestones (POA&M)** – plans of corrective actions that are designed to counter discovered risks and threats to the organization or organizational assets.
- **Risk** – the level of impact on organizational operations (including mission, functions, image or reputation), organizational assets or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
- **Risk Assessment** – the process of identifying risks to Agency operations (including mission, functions, image or reputation), Agency assets, individuals, other organizations and the Nation arising through the operation of the information system. Part of risk management, synonymous with risk analysis, incorporates threat and vulnerability analyses and considers mitigations provided by planned or in-place security controls.
- **Risk Management** – the process of managing risks to organizational operations (including mission, functions, image or reputation), organizational assets or individuals resulting from the operation of an information system, and includes:
  - The performance of a risk assessment.
  - The implementation of a risk mitigation strategy.
  - Employment of techniques and procedures for the continuous monitoring of the security state of the information system.
- **Security Categorization** – describes the potential adverse impacts to organizational operations, organizational assets and individuals should the information and information system be compromised through a loss of confidentiality, integrity or availability.
- **Security Controls** – safeguards or countermeasures that, when instituted, assist to avoid, counteract or minimize security risks.
- **Security Metrics** – the measurement of the effectiveness of security controls put inplace to secure organizational information and information systems.
- **Threat** – any circumstance or event with the potential to adversely impact Agency operations (including mission, functions, image or reputation), Agency assets or individuals through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial of service.
- **Vulnerability** – weakness in an information system, system security procedures, internal controls or implementation that could be exploited.
- **Vulnerability Assessment** – formal description and evaluation of an information system's vulnerabilities.

9. WAIVERS

Waivers or deviations may be requested through the EPA Risk Determination Process based on a substantive business need and the implementation of compensating controls that provide a suitable alternative to the mandated protection.

Only EPA's Chief Information Officer may authorize Agency-wide waivers or deviations from the standards herein.

10. DIRECTIVE(S) SUPERSEDED

This procedure supersedes Information Directive: CIO 2150-P-23.1 Information Security – Program Management Procedures, August 27, 2019.

11. CONTACTS

For 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: 2023.12.19 13:37:44 -05'00'

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

APPENDIX A: ACRONYMS & ABBREVIATIONS

APO	Agency Privacy Officer
CDO	Chief Data Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CPO	Chief Privacy Officer
CUI	Controlled Unclassified Information
EDMP	Enterprise Data Management Policy
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
IMO	Information Management Officer
IRMBC	Information Resource Management Branch Chief
ISO	Information Security Officer
IT	Information Technology
LPO	Liaison Privacy Official
MEF	Mission Essential Functions
NIST	National Institute of Standards and Technology
NPP	National Privacy Program
OGC	Office of General Counsel
OMB	Office of Management and Budget
PM	Program Management
PMEF	Primary Mission Essential Functions
POA&M	Plan of Action and Milestones
SAOP	Senior Agency Official for Privacy
SIO	Senior Information Official
SM	Service Manager
SO	System Owner
SP	Special Publication
U.S.C.	United States Code