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

Information Security – Planning (PL) 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 Planning (PL) 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
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004
- 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

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

NIST defines the applicable PL baseline controls in NIST 800-53B, *Control Baselines for Information Systems and Organizations*. The applicable security baseline for each impact level (Low, Moderate, High or For All Systems) as well as the Privacy Control Baseline are identified below the control name. EPA may deviate from the NIST 800-53B Security or Privacy Control Baselines by adding/removing controls or to applicable baselines and are notated with an asterisk.

PL-2 – System Security and Privacy Plans
For All Systems and Privacy Control Baseline:

1) Develop security and privacy plans for the system that:
   a) Are consistent with the organization's enterprise architecture;
   b) Explicitly define the constituent system components[1];
   c) Describe the operational context of the system in terms of mission and business processes;
   d) Identify the individuals that fulfill system roles and responsibilities;
   e) Identify the information types processed, stored, and transmitted by the system;
   f) Provide the security categorization of the system, including supporting rationale;
   g) Describe any specific threats to the system that are of concern to the organization;
   h) Provide the results of a privacy risk assessment for systems processing personally identifiable information (PII);
   i) Describe the operational environment for the system and any dependencies on or connections to other systems or system components;
   j) Provide an overview of the security and privacy requirements for the system;
   k) Identify any relevant control baselines or overlays, if applicable;
   l) Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;

[1] *System components include all networked devices, for example, mainframes, workstations, servers (e.g., database, electronic mail, authentication, Web, proxy, file, domain name), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors (e.g., Internet of Things (IoT) devices, robotic process automation (RPA) bots), operating systems, middleware, and applications (e.g., minor, major, tools and models).*

m) Include risk determinations for security and privacy architecture and design decisions;
n) Include security- and privacy-related activities affecting the system that require planning and coordination with the Office of Information Security and Privacy (OISP); and
o) Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.

2) Distribute copies of the plans and communicate subsequent changes to the ISO, Information System Security Officer (ISSO), Information Management Officer (IMO), Liaison Privacy Official (LPO), Information Resource Management Branch Chief (IRMBC) and ensure the latest version is uploaded as an artifact in the EPA Governance, Risk and Compliance (GRC) tool;
3) Review the plans annually or when there are significant changes[2] occurring to the system such as, major upgrade to operating system (OS) or critical software; or change in the operating environment, e.g. moving from on-premise to cloud (or vice versa), additions or reductions to the data or information types, or shifting to a hybrid model.
4) Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and
5) Protect the plans from unauthorized disclosure and modification.

PL-4 – Rules of Behavior

For All Systems and Privacy Control Baseline:

1) Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;
2) Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;
3) Review and update the rules of behavior annually or after changes to the system functionality or environment; and
4) Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge when the rules are modified.

PL-4(1) – Rules of Behavior | Social Media and External Site/Application Usage Restrictions

For All Systems and Privacy Control Baseline:

1) Include in the rules of behavior, restrictions on:
   a) Use of social media, social networking sites, and external sites/applications;
   b) Posting organizational information on public websites; and
   c) Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

PL-8 – Security and Privacy Architectures

For Moderate and High Systems and Privacy Control Baseline:

1) Develop security and privacy architectures for the system that:

[2] *A significant change is one that is likely to affect the security state of the information system as defined in NIST SP 800-37, Revision 2.*

a) Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;
b) Describe the requirements and approach to be taken for processing personally identifiable information to minimize the risk to individuals;
c) Describe how the architectures are integrated into and support the enterprise architecture; and
d) Describe any assumptions about, and dependencies on, external systems and services;

2) Review and update the architectures annually or upon notification of changes to the architecture to reflect updates in the enterprise architecture; and
3) Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

PL-9 – Central Management

For Privacy Control Baseline:

1) Centrally manage the EPA-wide EPA Common Controls, which include common controls identified as fully inherited or hybrid for only the enterprise EPA-wide responsibility part of the control, that would be available for all EPA information systems.

PL-10 – Baseline Selection

For All Systems:

1) Select a control baseline for the system.

PL-11 – Baseline Tailoring

For All Systems:

1) Tailor the selected control baseline by applying specified tailoring actions.

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

- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures

8. DEFINITIONS

- **Assessment** – See Security Control Assessment.
- **Compensating Control** – A management, operational, or technical control employed by a system in lieu of a recommended security control in the low, moderate or high baselines described in NIST SP 800-53 (as amended), which provides equivalent or comparable protection for a system.

- **Information Security** – The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability.
- **Organization** – A federal agency or, as appropriate, any of its operational elements.
- **Networked Devices** – IP-addressable networked assets that can be reached over IPv4 and IPv6 protocols. An IP-addressable networked asset is defined as any (i.e., non-ephemeral) information technology or operational technology asset that is assigned an IPv4 or IPv6 address and accessible over IPv4 or IPv6 networks, regardless of the environment in which it operates.
- **Privacy Impact Assessment (PIA)** – An analysis of how information is handled (i) to ensure handling conforms to applicable legal, regulatory and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
- **Security Control Assessment** – The testing and/or evaluation of the management, operational and technical security controls in a system to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for the system.
- **Security Requirements** – Requirements levied on a system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures or organizational mission/business case needs to ensure the confidentiality, integrity and availability of the information being processed, stored or transmitted.
- **Signature (of an individual)** – A mark or sign made by an individual to signify knowledge, approval, acceptance, or obligation (can be accomplished manually, sometimes referred to as a “wet signature,” or electronically).
- **System** – A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information.
- **System Security Plan (SSP)** – A formal document that provides an overview of the security and privacy requirements for the system and describes the security controls in place or planned for meeting those requirements.
- **User** – An individual or (system) process authorized to access a system.
- **Written (or in writing)** – Officially documenting the action or decision, either manually or electronically, and includes a signature.

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-2150.3-P-12.1 Information Security – Interim Planning Procedures, Version 3.6, July 17, 2012.

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 13:57:03 -05'00'

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

APPENDIX A: ACRONYMS & ABBREVIATIONS

CIO	Chief Information Officer
CISO	Chief Information Security Officer
CONOPS	Concept of Operations
EA	Enterprise Architecture
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
GRC	Governance, Risk and Compliance
IMO	Information Management Officer
IRMBC	Information Resource Management Branch Chief
ISO	Information Security Officer
ISSO	Information System Security Officer
NIST	National Institute of Standards and Technology
OISP	Office of Information Security and Privacy
OMB	Office of Management and Budget
OS	Operating System
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PL	Planning
SIO	Senior Information Official
SM	System Manager
SO	System Owner
SP	Special Publication
SSP	System Security Plan
U.S.C.	United States Code