For High-Impact Information Systems

FAMILY: PLANNING **CLASS:** MANAGEMENT

PL-1 SECURITY PLANNING POLICY AND PROCEDURES - The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.

PL-1.1 - Examine security planning policy and procedures; other relevant documents or records, **and**

Interview organizational personnel with information system security planning and plan implementation responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization develops and documents security planning policy and procedures.				
(ii)	The organization disseminates security planning policy and procedures to appropriate elements within the organization.				
(iii)	Responsible parties within the organization periodically review security planning policy and procedures.				
(iv)	The organization updates security planning policy and procedures when organizational review indicates updates are required.				

PL-1.2 - Examine security planning policy and procedures; other relevant documents or records, **and**

Interview organizational personnel with information system security planning and plan implementation responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The security planning policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance.				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(ii)	The security planning policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance.				
(iii)	The security planning procedures address all areas identified in the security planning policy and address achieving policy-compliant implementations of all associated security controls.				

PL-2 SYSTEM SECURITY PLAN - The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.

PL-2.1 - Examine security planning policy; procedures addressing information system security plan development and implementation; NIST Special Publication 800-18; security plan for the information system; other relevant documents or records, **and**

Interview organizational personnel with information system security planning and plan implementation responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization develops and implements a security plan for the information system.				
(ii)	The security plan provides an overview of the security requirements for the information system and a description of the security controls planned or in place for meeting the security requirements.				
(iii)	The security plan is consistent with NIST Special Publication 800-18.				
(iv)	The security plan is consistent with the organization's information system architecture and information security architecture.				
(v)	Designated organizational officials review and approve the security plan.				

PL-3 SYSTEM SECURITY PLAN UPDATE - The organization reviews the security plan for the information system [Assignment: organization-defined frequency, at least annually] and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.

PL-3.1 - Examine security planning policy; procedures addressing information system security plan reviews and updates; information system security plan (for organization-defined frequency for security plan updates); configuration management policy and procedures; configuration management documents; security plan for the information system; record of security plan reviews and updates; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines the frequency of information system security plan reviews and updates.				
(ii)	The organization updates the security plan in accordance with organization-defined frequency, at least annually				
(iii)	The organization receives input to update the security plan from the organization’s configuration management and control process.				
(iv)	The updated security plan reflects the information system and organizational changes or problems identified during the implementation of the plan or the assessment of the security controls.				

PL-4 RULES OF BEHAVIOR - The organization establishes and makes readily available to all information system users, a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.

PL-4.1 - Examine security planning policy; procedures for the development and implementation of rules of behavior for information system users; NIST Special Publication 800-18; rules of behavior; other relevant documents or records, **and**

Interview organizational personnel who are authorized users of the information system and have signed rules of behavior to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization establishes a set of rules that describe user responsibilities and expected behavior with regard to information system usage.				
(ii)	The organization makes the rules available to all information system users.				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(iii)	The rules of behavior for organizational personnel are consistent with NIST Special Publication 800-18.				
(iv)	The organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.				

PL-5 PRIVACY IMPACT ASSESSMENT - The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.

PL-5.1 - Examine security planning policy; procedures for conducting privacy impact assessments on the information system; appropriate federal legislation and OMB policy; privacy impact assessment; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.				
(ii)	The privacy impact assessment is consistent with federal legislation and OMB policy.				

PL-6 SECURITY-RELATED ACTIVITY PLANNING - The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.

PL-6.1 - Examine security planning policy; procedures for planning security-related activities for the information system; other relevant documents or records, **and**

Interview organizational personnel with information system security planning and plan implementation responsibilities to determine if the following requirements are met:

Requirement	S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations, organizational assets, and individuals.				
(ii)	The organization's advance planning and coordination of security-related activities includes both emergency and non-emergency situations.				