For High-Impact Information Systems

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES - The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, incident response 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 incident response policy and associated incident response controls.

IR-1.1 - Examine incident response policy and procedures; other relevant documents or records

and

Interview organizational personnel with incident response planning and plan implementation responsibilities to determine if the following requirements have been met:

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

IR-1.2 - Examine incident response policy and procedures; other relevant documents or records **and**

Interview organizational personnel with incident response planning and plan implementation responsibilities to determine if the following requirements have been met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The incident response policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among				

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

IR-2 INCIDENT RESPONSE TRAINING - The organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training [Assignment: organization-defined frequency, at least annually].

IR-2.1 - Examine incident response policy; procedures addressing incident response training; incident response training material; information system security plan (for organization-defined frequency for refresher incident response training); incident response training records; other relevant documents or records; **and**

Interview organizational personnel with incident response training and operational 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 identifies and documents personnel with incident response roles and responsibilities.				
(ii)	The organization provides incident response training to personnel with incident response roles and responsibilities.				
(iii)	Incident response training material addresses the procedures and activities necessary to fulfill identified organizational incident response roles and responsibilities.				
(iv)	The organization defines the frequency of refresher incident response training.				
(v)	The organization provides refresher incident response training in accordance with organization-defined frequency, at least annually.				

IR-3 INCIDENT RESPONSE TESTING AND EXERCISES - The organization tests and/or exercises the incident response capability for the information system [Assignment: organization-defined frequency, at least annually] using [Assignment: organization-defined tests and/or exercises] to determine the incident response effectiveness and documents the results.

IR-3.1 - Examine incident response policy; procedures addressing incident response testing and exercises; information system security plan (for list of organization-defined tests/exercises and organization-defined frequency of incident response tests/exercises); incident response testing material; incident response test results; 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 incident response tests/exercises.				
(ii)	The organization defines the frequency of incident response tests/exercises.				
(iii)	The organization tests/exercises the incident response capability for the information system using organization-defined tests/exercises in accordance with organization-defined frequency.				
(iv)	The organization documents the results of incident response tests/exercises.				

IR-4 INCIDENT HANDLING - The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

IR-4.1 - Examine incident response policy; procedures addressing incident handling capability; NIST Special Publication 800-61; other relevant documents or records, **and**

Interview organizational personnel with incident handling 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 implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.				
(ii)	The incident handling capability is consistent with NIST Special Publication 800-61.				

and

Test incident handling capability for the organization.

IR-4(1).1 - Examine incident response policy; procedures addressing incident handling capability; automated mechanisms supporting incident handling; other relevant documents or records to determine if the following requirements have been met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization employs automated mechanisms to support the incident handling process.				

IR-5 INCIDENT MONITORING - The organization tracks and documents information system security incidents on an ongoing basis.

IR-5.1 - Examine incident response policy; procedures addressing incident monitoring capability; incident response records and documentation; other relevant documents or records **and**

Interview organizational personnel with incident monitoring responsibilities to determine if the following requirements have been met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization tracks and documents information system security incidents on an ongoing basis.				

and

Test incident monitoring capability for the organization.

Test Steps		S	N	Findings	Initials & Date
1					

IR-6 INCIDENT REPORTING - The organization promptly reports incident information to appropriate authorities.

IR-6.1 - Examine incident response policy; procedures addressing incident reporting; NIST Special Publication 800-61; incident reporting records and documentation; other relevant documents or records, **and**

Interview organizational personnel with incident reporting 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 promptly reports incident information to appropriate authorities.				
(ii)	Incident reporting is consistent with NIST Special Publication 800-61.				
(iii)	The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.				
(iv)	Weaknesses and vulnerabilities in the information system are reported to appropriate organizational officials in a timely manner to prevent security incidents.				

and

Test incident reporting capability for the organization.

Test Steps		S	N	Findings	Initials & Date
1					

IR-6(1).1 - Examine incident response policy; procedures addressing incident reporting; automated mechanisms supporting incident reporting; other relevant documents or records **and**

Interview organizational personnel with incident reporting responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization employs automated mechanisms to assist in the reporting of security incidents.				

IR-7 INCIDENT RESPONSE ASSISTANCE - The organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the organization's incident response capability.

IR-7.1 - Examine incident response policy; procedures addressing incident response assistance; other relevant documents or records, **and**

Interview organizational personnel with incident response assistance and support 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 provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents.				
(ii)	The incident response support resource is an integral part of the organization's incident response capability.				

IR-7(1).1 - Examine incident response policy; procedures addressing incident response assistance; automated mechanisms supporting incident response support and assistance; other relevant documents or records **and**

Interview organizational personnel with incident response support and assistance responsibilities and organizational personnel that require incident response support and assistance to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization employs automated mechanisms to increase the availability of incident response-related information and support for incident response support.				