COMPUTER SECURITY INCIDENT RESPONSE POLICY

1 Overview

The Federal Information Security Management Act (FISMA) of 2002 requires Federal agencies to establish computer security incident response capabilities. Each Federal civilian agency must designate a primary and secondary point of contact (POC) with the United States Computer Emergency Response Team (US-CERT), report all incidents, and internally document corrective actions and their impact. OMB has also required reporting any release of personally identifiable information (PII), either in electronic or physical form, where that information may be accessed by those without a need to know the information. Each agency must determine how to best meet these requirements.

A computer security incident is any observable occurrence in a system, network, or any other electronic device or component that results in, or has the potential to result in a negative consequence, such as system crashes, network packet floods, unauthorized use of system privileges, defacement of a Web page, execution of malicious code that destroys data, or loss/theft of computer equipment or media.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, Computer Security Incident Handling Guide describes a computer security incident as a violation or imminent threat there of computer security policies or standard security practices. Examples of recent computer security incidents are as follows:

- Information Release
  - Information is placed onto a network or device that permits those without a need to know or authority to access the information.
  - Placements of Safeguards or Classified information onto the Internet, NRC's infrastructure, or computers unapproved to process this information and without adequate protections and restrictions.
- Denial of Service
  - An attacker sends specially crafted network transmissions to a Web server, causing it to crash.
  - An attacker directs hundreds of external compromised workstations to send as many Internet Control Message Protocol (ICMP) requests as possible to the organization's network.
- Malicious Code
  - A worm uses open file shares to quickly infect several hundred workstations within an organization.
  - An organization receives a warning from an antivirus vendor that a new virus is spreading rapidly via e-mail throughout the Internet. The virus takes advantage of a vulnerability that is present in many of the organization's hosts. Based on previous antivirus incidents, the organization expects that the new virus will infect some of its hosts within the next three hours.

- Unauthorized Access
  - An attacker runs an exploit tool to gain access to a server's password file.
  - A perpetrator obtains unauthorized administrator-level access to a system and then threatens the victim that the details of the break-in will be released to the press if the organization does not pay a designated sum of money.
  - An attacker uses social engineering to obtain a user's ID and password to gain access to a database containing sensitive information.
- Inappropriate Usage
  - A user provides illegal copies of software to others through peer-to-peer file sharing services.
  - A person threatens another person through e-mail.

Computer security incident response has become an important component of Information Technology (IT) programs. Security-related threats have become not only more numerous and diverse but also more damaging and disruptive. New types of computer security-related incidents emerge frequently. Preventative activities based on the results of risk assessments can lower the number of computer security incidents, but not all computer security incidents can be prevented. Therefore, a computer security incident response capability is necessary for proactively identifying potential threats (such as a new virus), rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. Computer security incident response is a team effort requiring strong coordination between all parties involved in the process.

Because effective computer security incident response is complex, establishing a successful incident response capability requires substantial planning and resources. Continually monitoring threats through Intrusion Detection Systems (IDS) and other mechanisms is essential. Establishing clear procedures for assessing the current and potential business impact of computer security incidents is critical, as is implementing effective methods of collecting, analyzing, and reporting data regarding those incidents. Building relationships and establishing suitable means of communication with other internal groups, such as the Office of Human Resources, Office of the Inspector General (OIG), and Office of the General Counsel (OGC) and with external groups, such as other incident response teams and law enforcement are also vital.

2 Purpose

This document provides Nuclear Regulatory Commission's (NRC) policy for responding to computer security incidents affecting NRC's infrastructure, networks, and users.

3 Scope

This policy applies to all NRC employees, contractors, vendors, and agents (users) having access to any system that processes NRC information, that resides at NRC facility or contractor

facility, having access to the NRC network, or storing of any public or non-public NRC information.

This policy also applies to all IT systems operated by the NRC, or operated by a contractor or outside entity on behalf of the NRC. In addition, this policy applies to all PII in all forms (either electronic or physical form).

4 Policy

This section provides the NRC policy for NRC computer security incident response, including all NRC systems or systems that process NRC information.

4.1 Computer Security Incident Response Plan (CSIRP)

The Cyber Situational Awareness, Analysis, and Response (CSAAR) Senior Information Technology Security Officer (SITSO) is responsible for ensuring development of a Computer Security Incident Response Plan (CSIRP) that includes but is not limited to:

- Standards for prioritizing computer security incidents. Computer security incidents should be prioritized based on the criticality of the affected resources and the effect the incident has on the organization. Response expectations should be set by priority level. For example: The Computer Security Incident Response Capability (CSIRC) must respond to a high priority computer security incident within 4 hours.
- Organization's computer security incident response process:
  - Preparation (selecting tools, preparing for computer security incidents, and preventing incidents)
  - Detection and Analysis (computer security incident categories, signs of an incident, sources of precursors and indications, incident analysis, incident documentation, incident prioritization, and incident notification)
  - Containment (containment strategy, evidence gathering and handling, identifying the attacker)
  - Eradication (deleting malicious code, disabling breached user accounts)
  - Recovery (restoring the system to normal operation and hardening the system to prevent similar computer security incidents)
  - Post Incident Activity (lessons learned, using collected incident data, evidence retention, assessing residual risk)
  - Recommendations for Improvement
- Compliance with Incident Reporting guidelines as identified at www.uscert.gov/federal

4.2 Computer Security Incident Response Team (CSIRT)

The CSIRC is provided by the Computer Security Office (CSO) and includes a centralized Computer Security Incident Response Team (CSIRT) that can assemble resources as needed from appropriate parts of NRC. The computer security incident response team leader and backup team leader are dedicated staff whose primary purpose is to address computer security incidents.

The CSIRT is staffed by the:

- CSO
- Office of Information Services (OIS);
- Office of Administration (ADM) Division of Facilities and Security; and
- Office of Nuclear Security and Incident Response (NSIR) Information Security representatives.

The CSIRT responsibilities are a higher priority for the CSO and OIS team members than their other duties. Staff from NSIR and ADM will be made available in an expeditious manner to support the CSIRT efforts. The CSIRT receives specialized training annually, including simulated events, to facilitate an effective response by personnel during crisis situations. As appropriate, annual training will use automated mechanisms to provide a more robust and realistic training environment, where possible.

4.3 Computer Security Incident Reporting

The CSIRT is responsible for developing a report summarizing all computer security incidents and all PII incidents (whether the compromise was electronic or physical), transmitting this report to the CSAAR SITSO and Chief Information Security Officer (CISO) for approval, and notifying US-CERT about malicious or suspicious activity. Computer security incidents are reported to US-CERT based upon federal incident reporting guidelines and standards.

All potential or confirmed incidents involving PII must be reported to the NRC senior agency official for privacy (Deputy Chief Information Officer) and to US-CERT within 1 hour of discovery, and all known or suspected instances of spillages of classified information must be promptly reported.

Classified Computer Security incidents must follow Committee on National Security System (CNSS) polices including but not limited to CNSS Policy No. 18 and CNSS Institution No. 1001 February 2002.

4.3.1 Cyber Situational Awareness, Analysis, and Response (CSAAR) Senior Information Technology Security Officer (SITSO)

The CSAAR SITSO provides a recommendation to the Chief Information Security Officer (CISO) whether or not law enforcement or the OIG is needed to address a computer security incident. Also, the CSAAR SITSO is responsible for testing the CSIRC annually to determine its effectiveness and documenting those results. When possible, the CSAAR SITSO's evaluation of the organization's computer security incident response capability employs automated mechanisms to more thoroughly test the organization's incident handling process.

4.3.2 NRC Customer Support Center

The NRC Customer Support Center (CSC or Helpdesk) is responsible for reporting any actual or potential computer security incidents and all actual or potential PII incidents when they are recognized. A computer security or PII incident, verified or suspected, must be immediately reported to the NRC CSIRT. Prompt reporting of a suspected incident is essential in limiting damage resulting from the incident. The CSIRT can be contacted directly at 301-415-6666 or CS_IRT@nrc.gov.

5 Responsibilities

This section summarizes the roles and responsibilities for responding to and reporting computer security incidents.

5.1 Computer Security Incident Response Team (CSIRT)

The CSIRT responsibilities include the following:

- Immediately notifies the CSAAR SITSO and CISO of any computer security or PII incident.
- Immediately notifies the NRC senior agency official for privacy of any PII incident.
- Recommends to the CSAAR SITSO if law enforcement or OIG involvement is needed to address a computer security incident.
- Reports computer security incidents within the time frames required by federal guidance directly to external groups such as US-CERT or law enforcement if NRC management is unavailable to give their approval. The NSIR operations center will be asked to assist in contacting management if the CSIRT has difficulty. Law enforcement contact will be made through standard channels if at all possible.
- Notifies the CISO (if CSAAR SITSO is not available to do so) if law enforcement or OIG is contacted.
- Develops and maintains procedures for computer security incident handling and reporting based on NRC's CSIRT policy.
- Is available to respond 24 hours a day, 7 days a week, and 365 days a year.

- Develops and maintains standards to ensure that an adequate audit trail exists to support the organization's computer security incident handling process.
- Develops and maintains guidelines for communicating with outside parties regarding computer security incidents.
- Develops and maintains a best practices knowledge base for resolving various computer security incidents.
- Incorporates lessons learned from ongoing incident handling activities into the organization's computer security incident handling process.
- Confiscates or disconnects equipment as required to prevent additional computer security incidents or damage to NRC systems, and monitors suspicious activity throughout the NRC.
- Employs automated mechanisms to support the computer security incident handling process, to support the tracking of security incidents, to assist in the collection of computer security incident information, to assist in the analysis of computer security incident information, and to help with the reporting of computer security incidents.
- Develops and maintains guidelines for communicating computer security incident response information with outside parties.
- Establishes and maintains relationships with internal organizations (e.g., General Counsel) and external groups (e.g., Department of Homeland Security).
- Tracks and documents computer security incidents on an ongoing basis (24/7 365 days a year).
- Develops and maintains audit trail standards and procedures.
- The CSIRT team leader is responsible for ensuring these responsibilities are fulfilled.

5.2 Cyber Situational Awareness, Analysis, and Response (CSAAR) Senior IT Security Officer (SITSO)

- Provides oversight and guidance for the organization's computer security incident response process.
- Develops and maintains a CSIRC based on Federal regulations, standards, and guidelines.
- Raises any issues with the organization's computer security incident response process with the CISO.
- Oversees all CSIRC activities.
- Reviews and approves all formal policies, procedures and best practices relating to computer security incident response.
- Reviews and approves all incident reports if the computer security incident has been prioritized as moderate or high.

- Reviews and approves all routine periodic computer security incident response reports before they are sent to the CISO, or other Federal agencies.
- Evaluates all computer security incidents and makes a recommendation to the CISO if the involvement of law enforcement or OIG is needed.
- Decides if the involvement of law enforcement or OIG is necessary to mitigate the computer security incident, if the CISO is not available to do so.
- Notifies the CIO if law enforcement or OIG is contacted, if the CISO is not available to do so.
- Tests and documents the computer security incident response capability annually to determine the capabilities' effectiveness.

5.3 Chief Information Security Officer (CISO)

- Ensures all computer security incident response issues raised by the CSAAR SITSO are addressed.
- Reviews periodic computer security incident response reports.
- Reviews all computer security incident response reports sent to other Federal agencies.
- Reviews and approves all computer security incident reports if the incident has been prioritized as high.
- Decides if the involvement of law enforcement or OIG is necessary to mitigate the computer security incident.
- Decides whether or not to allow the operation of an information system after a high-level computer security incident has occurred.
- Approves the computer security incident response procedures used by the agency.
- Notifies the CIO if law enforcement or OIG is contacted.
- Notifies the CIO if appropriate due to the nature of the incident.
- Notifies the Executive Director for Operations (EDO), Office of Public Affairs (OPA), and Commission if appropriate and the CIO is unavailable to do so.

5.4 Chief Information Officer (CIO)

- Notifies the EDO, OPA, and Commission if appropriate due to the nature of the incident.

5.5 Customer Support Center (Helpdesk)

- Analyzes and evaluates incoming calls for malicious or suspicious activity
- Notifies the NRC CSIRT immediately if malicious or suspicious activity has been identified.

6.6 Users

Users should refer to the NRC rules of behavior for their incident response responsibilities.

6 Enforcement

The Office of Human Resources provides the policy for disciplinary action for violations of IT security policies and procedures.

7 Frequency of Review

The Computer Security Policy, Standards, and Training (CSPST) SITSO is responsible for reviewing this policy at least annually.

8 Cognizant Authority

The CSPST SITSO is responsible for maintaining this policy.