Cyber Security Technical and Management Requirements

Incident Management (TMR-9)
October 10, 2007

Department of Energy (DOE) Order 205.1A, *Department of Energy Cyber Security Management*, charges Senior DOE Management to implement cyber security within their respective organizations, based on their determination, assessment, and documentation of DOE and program-unique threats and risks. In carrying out this charge, Senior DOE Management is required by the Order to develop a Program Cyber Security Plan (PCSP) that defines cyber security requirements for all subordinate organizations and programs. The Order requires that the PCSP requirements comply with the Federal Information Security Management Act (FISMA), Presidential directives and Executive orders, Office of Management and Budget (OMB) directives, Federal Information Processing Standards (FIPS), Departmental policies, and DOE Chief Information Officer (CIO) Cyber Security Technical and Management Requirements (TMRs). This TMR document provides Senior DOE Management general direction and minimum requirements for unclassified and National Security Systems to be used in preparing each PCSP.

This TMR defines a structured, cohesive, and consistent process for identifying, containing, reporting, and mitigating information security incidents involving DOE Federal information systems that is to be covered in each PCSP. It also provides guidance for the Departmental implementation of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, *Computer Security Incident Handling Guide*, Office of Management and Budget Memoranda, and applicable Departmental and Federal information technology security laws and regulations. The requirements of this TMR are in addition to those outlined by DOE M 470.4-1, *Safeguards and Security Program Planning and Management,* and do not relieve any organization from the requirements for incident management as outlined by that DOE Directive. Senior DOE Management may specify and implement additional requirements in each PCSP to address specific risks, vulnerabilities, or threats within its operating units.

Cancellations

This TMR replaces DOE CIO Guidance CS-9, *Incident Management Guidance,* dated January 2007.

Implementation

This document defines management and technical cyber security requirements to be incorporated into Senior DOE Management PCSPs within 90 days of the TMR issue date.

Requirements

TMR-9-1, Senior DOE Management Incident Management Policy

Senior DOE Management is responsible for developing, documenting in the PCSP, and implementing incident management policies for all operating units, programs, and systems. At a minimum, the Senior DOE Management PCSP is to address:

1. Training for users, system administrators, and cyber security staff in incident reporting and handling procedures.

2. Incident and potential incident management procedures.

3. Impact assessment for every cyber security incident.

4. Incident categorization and documentation.

5. Timely reporting of incidents and maintenance of incident records.

6. Integration of incident handling processes with Personally Identifiable Information (PII) incident reporting, Information Condition (INFOCON) processes, Contingency Plans for each information system, and Contingency Plan testing.

7. Handling information and cyber alerts disseminated by the Computer Incident Advisory Capability (CIAC).

TMR-9-2, Alerts and Incident Categorization and Impact Assessment

The Senior DOE Management PCSP must document incident management processes, policies, and procedures to categorize and assess incident impact for all operating units, programs, and systems. At a minimum, the PCSP is to address the criteria as follows:

1. Characterize and categorize cyber security incidents according to their potential to cause harm to information and information systems based on two criteria: Incident Type and Incident Category. These criteria are used to determine the time frame for reporting incidents to the CIAC (http://www.ciac.org/ciac/index.html).

    a. Incident Types.

        (1) Type 1 incidents are successful incidents that potentially create serious breaches of DOE cyber security or have the potential to generate negative media interest. The following are defined as Type 1 incidents, and all are to be reported.

            (a) System Compromise/Intrusion. All unintentional or intentional instances of system compromise or intrusion by unauthorized persons, including user-level compromises, root (administrator) compromises, and instances in which users exceed privilege levels.

(b) Loss, Theft, or Missing. All instances of the loss of, theft of, or missing laptop computers; and all instances of the loss of, theft of, or missing information technology resources, including media that contained Sensitive Unclassified Information (SUI) or national security information.

(c) Web Site Defacement. All instances of a defaced Web site.

(d) Malicious Code. All instances of successful infection or persistent attempts at infection by malicious code, such as viruses, Trojan horses, or worms.

(e) Denial of Service. Intentional or unintentional denial of service (successful or persistent attempts) that affects or threatens to affect a critical service or denies access to all or one or more large portions of a network. Critical services are determined through Business Impact Analyses in the Contingency Planning process.

(f) Critical Infrastructure Protection (CIP). Any activity that adversely affects an asset identified as critical infrastructure. CIP assets are identified through the Contingency Planning process.

(g) Unauthorized Use. Any activity that adversely affects an information system's normal, baseline performance and/or is not recognized as being related to Senior DOE Management mission is to be reported. Unauthorized use includes, but is not limited to, port scanning that excessively degrades performance; IP (Internet protocol) spoofing; network reconnaissance; monitoring; hacking into DOE servers and other non-DOE servers; running traffic-generating applications that generate unnecessary network broadcast storms or drive large amounts of traffic to DOE computers; or using illegal (or misusing copyrighted) software images, applications, data, and music. Unauthorized use can involve using DOE systems to break the law.

(h) Information Compromise. Any unauthorized disclosure of information that is released from control to entities that do not require the information to accomplish an official Government function such as may occur due to inadequate clearing, purging, or destruction of media and related equipment or transmitting information to an unauthorized entity or transmitting information over a network not authorized for the information (e.g., classified on an unclassified network, SUI over the Internet, etc).

(2) Type 2 incidents are attempted incidents that pose potential long-term threats to DOE cyber security interests or that may degrade the overall effectiveness

of the Department's cyber security posture. The following are the currently defined Type 2 incidents.

(a) Attempted Intrusion. A significant and/or persistent attempted intrusion is an exploit that stands out above the daily activity or noise level and would result in unauthorized access (compromise) if the system were not protected.

(b) Reconnaissance Activity. Persistent surveillance and resource mapping probes and scans are those that stand out above the daily activity or noise level and represent activity that is designed to collect information about vulnerabilities in a network and to map network resources and available services. The Senior DOE Management PCSP must document the parameters for collecting and reporting data on surveillance probes and scans.

b. Incident Categories. Incident Categories characterize the potential impact of incidents that compromise DOE information and information systems. Such incidents may impact national security, DOE operations, assets, individuals, mission, or reputation. Incident categories identify the level of sensitivity and criticality of information and information systems by assessing the impact of the loss of confidentiality, integrity, and availability. Each of the security objectives—confidentiality, integrity, and availability—is assessed in the following manner.

(1) Low Incident Category. Loss of system confidentiality, integrity, or availability could be expected to cause damage to national security or have a limited adverse effect on DOE operations, assets, or individuals, including loss of secondary mission capability, requiring minor corrective actions or repairs.

(2) Moderate Incident Category. Loss of system confidentiality, integrity, or availability could be expected to cause serious damage to national security or have a serious adverse effect on DOE operations, assets, or individuals, including significant degradation, non-life threatening bodily harm, loss of privacy, or major damage, requiring extensive corrective actions or repairs.

(3) High Incident Category. Loss of system confidentiality, integrity, or availability could be expected to cause serious effect to national security or have a severe or catastrophic adverse effect on DOE operations, assets, or individuals. The incident could pose a threat to human life, cause the loss of mission capability, or result in the loss of major assets.

(4) Very High Incident Category. Loss of system confidentiality, integrity, or availability could be expected to cause grave damage to national security.

2. Complete incident reports in a timely manner, and maintain all records. Incident management processes and procedures are included in Contingency Plan testing and integrated with PII incident reporting, INFOCON processes and procedures, and each information system Contingency Plan.

   a. When a cyber security incident has occurred or is suspected to have occurred (potential incident), the affected site will immediately examine and document the pertinent facts and circumstances surrounding the event.

   b. The initial investigation of an event is completed within 24 hours. If the initial investigation of a potential incident cannot be completed within 24 hours, an initial report must be made as soon as possible but no later than 2 hours from the end of the 24-hour time period.

   c. Once it is determined that an incident has occurred, the incident must be categorized according to Incident Type and Incident Category, analyzed for impact to Senior DOE Management operations, and reported to CIAC within the time frames indicated in Table 1. All reporting timeframes begin at discovery of the potential incident

   d. All potential incident evaluations and incidents must be documented and local files retained.

Table 1. Required Time Frame for Reporting Cyber Security Incidents to the Computer Incident Advisory Capability

	Incident Category				
Incident Type	Low	Moderate	High		Very High
Type 1	Within 4 hours	Within 2 hours	Within 1 hour	PII within 45 minutes	Within 1 hour
Type 2	Within 1 week	Within 48 hours	Within 24 hours		Within 8 hours

   e. A monthly report to CIAC on the status of incident resolution is required from all operating units whether or not any successful or attempted cyber security incidents have occurred during the previous month.

   f. The Office of Health, Safety, and Security must be informed of all incidents involving National Security Systems in accordance with the requirements of DOE M 470.4-1, *Safeguards and Security Program Planning and Management*.

   g. Automated systems may be used for reporting if reporting by such systems complies with PCSP requirements.

3. Develop, document, and implement procedures for handling information disseminated by CIAC and responding proactively to alerts, performing consequence analyses, and performing corrective actions. CIAC is the official DOE point of contact for prompt dissemination of information provided in alerts received from external organizations. At a minimum, these procedures include:
    a. Acknowledge to CIAC the receipt of the alert by the operating unit within 4 normal business hours,
    b. Confirm the operating unit INFOCON is appropriate,
    c. Execute analyses relative to the activities described in the alert,
    d. Execute appropriate corrective actions; and
    e. Report the actions taken or provide justification for why actions were not taken.
4. Integrate incident management processes and procedures with each information system Contingency Plan and test incident response as part of Contingency Plan testing. Incident response capability must be maintained during contingency conditions.
5. Develop and document an impact assessment process to evaluate each incident that, at a minimum, addresses on the following:
    a. Loss of information confidentiality, integrity, and/or availability
    b. Intelligence value
    c. Impacts on business continuity
    d. Legal, ethical, or privacy (Human Resources) issues
    e. Impact on current or future operations of the DOE, facility or Project/Program
    f. Cost impacts (e.g., cost of resolution, productivity loss, etc)
    g. Current and potential technical effects
    h. Criticality of affected resources
    i. Impacts on confidence and reputation of DOE, facility, or program/project

TMR-9-3, Cyber Security Incidents Involving Personally Identifiable Information.
The Senior DOE Management PCSP is to document policies and procedures for managing incidents involving PII for all operating units, programs, and systems. At a minimum, the PCSP is to address the following:

1. Establish and document procedures for reporting cyber security incidents and potential incidents related to PII in accordance with the processes and time frames outlined in this TMR.

2. Validate that there is sufficient reason to believe that a security breach has occurred and that PII is likely to have been involved. Otherwise, the incident should be reported following documented procedures for reporting all cyber security incidents.

3. Develop processes to notify the Information Owner/Data Steward once it has been determined that confidentiality of PII has been compromised.

4. Ensure that all suspected or confirmed cyber security incidents involving media containing PII (including the physical loss/theft of computing devices) are reported to CIAC within 45 minutes of discovery. CIAC will report to the US-Computer Emergency Readiness Team (US-CERT) in accordance with its procedures.

5. Report to CIAC via the CIAC AWARE portal, or alternatively by email to ciac@ciac.org, phone to 925-422-8193, or fax to 925-423-8002.

TMR-9-4, Cyber Incident Response Plan

The Senior DOE Management PCSP is to specify the requirements for preparation of a Cyber Incident Response Plan for all operating units, programs, and systems. At a minimum, the plan is to include the following.

1. Procedures for cyber incident reporting, investigation, mitigation including emergency patch installation, forensics, evidence gathering, formal incident reporting, and impact assessment.

2. Formal incident reporting procedures for reports to CIAC and receiving reports of potential incidents from users.

3. Roles and responsibilities for the Cyber Incident Response Team (CIRT), to include emergency points-of-contact.

    a. The CIRT core group should include a CIRT Leader, a member with an investigative or forensics background, a representative from the Office of the Inspector General (OIG), a representative from Human Resources, and a representative from Public Relations.

    b. Expertise available to the CIRT on an "on-call" basis should include system administration, network administration, database administration, Information System Security Officers, and cyber forensics to assist the core group with the investigation and mitigation of the incident.

    c. The CIRT members are to be trained in incident investigation, formal reporting, and mitigation techniques appropriate to their role in the Cyber Incident Response Plan.

4. Provisions to assist and support Inquiry Officials under DOE M 470.4-1, *Safeguards and Security Program Planning and Management* in the conduct of inquiries.

TMR-9-5, Cyber Incident Records

The Senior DOE Management PCSP is to specify the requirements for maintaining Cyber Incident Records by all operating units, programs, and systems. At a minimum, the records for incidents and potential incidents are maintained, archived, and include the following:

1. Content requirements for reporting to CIAC (available from the CIAC Web site, http://www.ciac.org).

2. Additional report contents to include:
   a. Name of organization;
   b. Contact information for the incident;
   c. Physical location of affected computer/network;
   d. Date incident occurred;
   e. Time incident occurred;
   f. Which critical infrastructure was affected, if any;
   g. Type of incident (e.g., intrusion, denial of service, Web site defacement);
   h. Internet protocol (IP) address and domain name of affected system(s);
   i. IP address and domain name of apparent attacker(s);
   j. Operating system of affected host(s);
   k. Functions of affected host(s);
   l. Number of hosts affected;
   m. Suspected method of intrusion/attack;
   n. Suspected perpetrators and/or possible motivations;
   o. Evidence of spoofing;
   p. Application software affected;
   q. What security infrastructure was in place;
   r. Whether the intrusion resulted in loss of sensitive information;

s. Whether the intrusion damaged the system(s);

t. What actions have been taken;

u. With whom the information can be shared (e.g., National Infrastructure Protection Center, National Security Incident Response Center);

v. Whether the OIG has been informed of the Type 1 incident;

w. Whether the local FBI office has been informed of the incident;

x. Whether any other agency has been informed, and if so, what its contact information is;

y. Last time the system(s) was modified or up; and

z. Assessment of the impact of the incident.

TMR-9-6, Operating Unit Policies and Procedures

The Senior DOE Management PCSP is to direct operating units to develop, document, and implement policies and procedures for incident management compliant with the requirements defined in the PCSP and commensurate with the level of security required for the organization's environment and specific needs.