

**U.S. Department of Energy
Cyber Security Program**

**INCIDENT MANAGEMENT
GUIDANCE**



January 2007

***This Guidance document was
developed and issued outside of the
Departmental Directives Program.***

1. PURPOSE.

This Department of Energy (DOE) Chief Information Officer (CIO) Guidance define a structured, cohesive, and consistent process for performing incident warning, and response (sometimes referred to collectively as incident management) for DOE Federal information systems, which include national security systems, and applies the principles and requirements of National Institute for Science and Technology Special Publication (NIST SP) 800-61, *Computer Security Incident Handling Guide*, and other applicable Departmental and Federal information technology security laws and regulations.

The purpose of this guidance is to establish incident reporting processes and local response processes solely for security incidents involving IT resources. The requirements of this guidance 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.

The DOE Office of the Chief Information Officer (OCIO) will review this Guidance annually and update it as necessary. The DOE Under Secretaries, the NNSA Administrator, the Energy Information Administration, the Power Marketing Administrations, and DOE Chief Information Officer (CIO) (hereinafter referred to as Senior DOE Management) and their subordinate organizations and contractors (hereinafter called operating units) may provide feedback at any time for incorporation into the next scheduled update.

2. SCOPE.

This Guidance is provided to Senior DOE Management for addressing the reporting of security incidents involving IT resources that are utilizing the controls in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance*, and DOE Manual 205.1-4, *National Security Systems Controls Manual*, in their Program Cyber Security Plans (PCSPs) to protect DOE/ Government information..

3. CANCELLATIONS.

None.

4. APPLICABILITY.

- a. Primary DOE Organizations. This Guidance applies to all DOE Organizations listed in Attachment 1, *Primary Department of Energy Organizations to Which DOE CIO Guidance CS-9 is Applicable*.

Further, Senior DOE Management may specify and implement supplemental requirements to address specific risks, vulnerabilities, or threats within their operating units, and for ensuring that those requirements are incorporated into contracts.

- b. Exclusions. Consistent with the responsibilities identified in Executive Order (E.O.) 12344, the Director of the Naval Nuclear Propulsion Program will ensure consistency through the joint Navy and DOE organization of the Naval Nuclear Propulsion Program and will implement and oversee all requirements and practices pertaining to this DOE Guidance for activities under the NNSA Administrator's cognizance.
- c. Unclassified Systems. Senior DOE Management PCSPs are to address this Guidance for all DOE systems hosting unclassified information. DOE CIO Guidance CS-38, *Protection of Personally Identifiable Information*, DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, and DOE M 471.1-1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual*, provide additional information for identifying unclassified information requiring protection.
- d. National Security Systems. Senior DOE Management PCSPs are to address this Guidance for all DOE National Security Systems. The protection mechanisms described in this guidance are consistent with and implement the policies and practices set forth by Executive Order 12829 (E.O. 12829), which established the National Industrial Security Program; the requirements of the *National Industrial Security Program Operating Manual (NISPOM)*; the Atomic Energy Act of 1954, which established Restricted Data information; and EO 12958, *Classified National Security Information*, which prescribes a uniform system for classifying, safeguarding, and declassifying national security information.. NIST SP 800-59, *Guidelines for Identifying an Information System as a National Security System*, provides additional guidance for identifying National Security systems.

5. IMPLEMENTATION.

This Guidance is effective 30 days after issuance. However, DOE recognizes that this Guidance cannot be implemented into Senior DOE Management PCSPs overnight. Except as noted below, DOE expects that Senior DOE Management shall address the criteria in this document within 90 days of its issuance. If Senior DOE Management cannot address all of the criteria by that date, Senior DOE Management is to establish a Plan of Actions and Milestones (POA&M) for implementation of this Guidance into their PCSPs.

6. CRITERIA.

- a. Senior DOE Management PCSPs must define policies, processes, and procedures for incident handling and response to include at least the following.

- (1) Personnel training in incident management procedures;
 - (2) Incident and potential incident reporting;
 - (3) Impact assessment for every cyber security incident;
 - (4) Incident categorization and documentation;
 - (5) Timely reporting of incidents, maintenance of incident records, and integration of incident handling processes with Personally Identifiable Information incident reporting, Information Condition (INFOCON) processes, Contingency Plans for each information system, and Contingency Plan testing;
 - (6) Handling information and cyber alerts disseminated by CIAC; and
 - (7) Application of Configuration Management to security patching and updating, including testing and reviewing for security significant change impacts and risk mitigation.
- b. Program Cyber Security Plan. Senior DOE Management PCSPs are to comply with the criteria in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance*, and DOE Manual 205.1-4, *National Security Systems Controls Manual*. Senior DOE Management PCSPs are to direct operating units to develop, document, and implement policies and procedures for incident management that comply with the following criteria and commensurate with the level of security required for the organization's environment and specific needs. Requirements for reporting incidents involving PII are included in Paragraph 6.c below.
- (1) Characterize and categorize cyber security incidents according to their potential to cause damage to information and information systems based on two criteria: Incident Type and Security Category. These criteria are used to determine the time frame for reporting incidents to the CIAC.
 - (a) Incident Types.
 - i. 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.
 - (i.) System Compromise/Intrusion. All unintentional or intentional instances of system compromise or intrusion by unauthorized persons must be reported, including user-level compromises, root (administrator) compromises, and instances in which users exceed privilege levels.

- (ii.) 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 IT resources, including media, that contained Sensitive Unclassified Information (SUI) or national security information.
- (iii.) Web Site Defacement. All instances of a defaced Web site must be reported.
- (iv.) Malicious Code. All instances of successful infection or persistent attempts at infection by malicious code, such as viruses, Trojan horses, or worms, must be reported.
- (v.) 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 must be reported. Critical services are determined through Business Impact Analyses in the Contingency Planning process.
- (vi.) Critical Infrastructure Protection (CIP). Any activity that adversely affects an asset identified as critical infrastructure must be reported. CIP assets are identified through the Contingency Planning process.
- (vii.) 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.
- (viii.) 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.

- ii. 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.
 - (i.) Attempted Intrusion. A significant and/or persistent attempted intrusion is an exploit that stands out above the daily activity or noise level, as determined by the system owner, and would result in unauthorized access (compromise) if the system were not protected.
 - (ii.) 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) Security Categories characterize the potential impact of incidents that compromise DOE information and information systems. Such incidents may impact DOE operations, assets, individuals, mission, or reputation. Security 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.
 - i. Low Security Category. Loss of system confidentiality, integrity, or availability could be expected to have a limited adverse effect on DOE operations, assets, or individuals, including loss of secondary mission capability, requiring minor corrective actions or repairs.
 - ii. Moderate Security Category. Loss of system confidentiality, integrity, or availability could be expected to 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.
 - iii. High Security Category. Loss of system confidentiality, integrity, or availability could be expected to 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.

- (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 Personally Identifiable Information incident reporting, Information Condition (INFOCON) processes and procedures, and each information system Contingency Plan. Additional requirements for reporting incidents involving PII are included in Paragraph 6.c below.
- (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 within 26 hours. Once it is determined that an incident has occurred, the incident must be categorized according to Incident Type and Security Category, analyzed for impact to Senior DOE Management operations, and reported to CIAC within the time frames indicated in Table 1, in accordance with the process established in the applicable PCSP.
 - (c) 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

	Security Category		
Incident Type	Low	Moderate	High
Type 1	Within 4 hours ¹	Within 2 hours	Within 1 hour
Type 2	Within 1 week	Within 48 hours	Within 24 hours

- (d) A monthly report on the status of incident resolution is to be required from all operating units whether or not any reportable successful or attempted cyber security incidents have occurred during the previous month.

¹ Reporting timeframes begin at the point of potential incident identification.

- (e) The Office of Health, Safety, and Security must be informed of all incidents involving National Security Systems in accordance with the requirements of DOE O 471.4-1, *Safeguards and Security Program Planning and Management*.
 - (f) 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 the receipt of the alert 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) Test and review cyber security patches and updates under Configuration Management procedures for security significant change impacts, risk mitigation, and new vulnerabilities. Security patches are to be installed in a timely manner. The Designated Approving Authority (DAA) must approve decisions not to apply security patches, as in the case where stability may be sacrificed (and thus availability). All patches and updates must be reviewed for site applicability, system risk mitigation, and tested to ensure new vulnerabilities are not introduced to the system. Patches may be obtained from a number of sources, including CIAC, the US-CERT Web site (<http://www.us-cert.gov>), and trusted vendors.
- (5) 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.
- (6) Develop and document an impact assessment for each reportable 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
- (7) Develop, document, and implement a Cyber Incident Response Plan. Each Cyber Incident Response Plan must include:
- (a) Procedures for cyber incident reporting, investigation, mitigation including emergency patch installation, forensics, evidence gathering, formal incident reporting, and impact assessment.
 - (b) Formal incident reporting procedures for reports to CIAC and receiving reports of potential incidents from users.
 - (c) Identify roles and responsibilities for the Cyber Incident Response Team (CIRT), to include emergency points-of-contact.
 - i. The CIRT core group should include a CIRT Leader, a member with an investigative or forensics background, a representative from the Inspector General’s office (OIG), a representative from the Human Relations (HR), and a representative from Public Relations (PR).
 - ii. 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.
 - iii. Avoid placing personnel performing the investigation into a conflict of interest position.
 - (d) Provisions are made to assist and support Inquiry Officials under DOE M 470.4-1, *Safeguards and Security Program Planning and Management* in the conduct of inquiries.

- (e) Records for incidents and potential incidents are maintained and archived.
- i. Incident report content requirements can be found at the CIAC Web site (www.ciac.org).
 - ii. In addition to the CIAC report, incident records are to include the following:
 - (i.) Name of organization;
 - (ii.) Contact information for the incident;
 - (iii.) Physical location of affected computer/network;
 - (iv.) Date incident occurred;
 - (v.) Time incident occurred;
 - (vi.) Which critical infrastructure was affected, if any;
 - (vii.) Type of incident (for example, intrusion, denial of service, Web site defacement);
 - (viii.) Internet protocol (IP) address and domain name of affected system(s);
 - (ix.) IP address and domain name of apparent attacker(s);
 - (x.) Operating system of affected host(s);
 - (xi.) Functions of affected host(s);
 - (xii.) Number of hosts affected;
 - (xiii.) Suspected method of intrusion/attack;
 - (xiv.) Suspected perpetrators and/or possible motivations;
 - (xv.) Evidence of spoofing;
 - (xvi.) Application software affected;
 - (xvii.) What security infrastructure was in place;
 - (xviii.) Whether the intrusion resulted in loss of sensitive information;

- (xix.) Whether the intrusion damaged the system(s);
- (xx.) What actions have been taken;
- (xxi.) With whom the information can be shared (for example, National Infrastructure Protection Center, National Security Incident Response Center);
- (xxii.) Whether the OIG has been informed of the Type 1 incident;
- (xxiii.) Whether the local FBI office has been informed of the intrusion;
- (xxiv.) Whether any other agency has been informed, and if so, what its contact information is; and
- (xxv.) Last time the system(s) was modified or up.
- (xxvi.) Assessment of the impact of the incident.

- (8) Train users, system administrators, and cyber security staff in incident handling procedures.
 - (a) The CIRT is trained in incident investigation, formal reporting, and mitigation techniques appropriate to their role in the Incident Response Plan.
 - (b) All users are provided incident reporting and handling training.
- c. Requirements for Reporting of Cyber Security Incidents Involving Personally Identifiable Information (PII). Senior DOE Management PCSPs are to direct operating units to develop, document, and implement policies and procedures for reporting incidents involving PII, in accordance with the following criteria.
 - (1) Establish, document, and implement procedures for reporting cyber security incidents related to PII in accordance with the processes and time frames outlined in this Guidance.
 - (2) Develop processes to notify the Information Owner once it has been determined that confidentiality of PII has been compromised.
 - (3) Ensure that all suspected or confirmed cyber security incidents involving media containing PII (including the physical loss/theft of computing devices) are reported to the DOE Cyber Incident Advisory Capability (CIAC) within 45 minutes of discovery. CIAC will report to the US-Computer Emergency Readiness Team (US-CERT) in accordance with its procedures.

- (4) When reporting possible cyber security incidents involving PII, there should be 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.
- (5) Reports to CIAC should be made via the CIAC AWARE portal, or alternatively by email to ciac@ciac.org, phone to 925-422-8193, or fax to 925-423-8002.

7. REFERENCES.

References are listed in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls*.

8. DEFINITIONS.

Definitions specific to this Guidance are included in Attachment 2. Acronyms and terms applicable to all DOE CIO Guidance are defined in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance*.

9. CONTACT.

Questions concerning this Guidance should be addressed to the Office of the Chief Information Officer, (202) 586-0166.

ATTACHMENT 1

PRIMARY DEPARTMENT OF ENERGY ORGANIZATIONS TO WHICH DOE
CIO GUIDANCE CS-9 IS APPLICABLE

Office of the Secretary
Office of the Chief Financial Officer
Office of the Chief Information Officer
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Departmental Representative to the Defense Nuclear Facilities Safety Board
Office of Economic Impact and Diversity
Office of Electricity Delivery and Energy Reliability
Office of Energy Efficiency and Renewable Energy
Energy Information Administration
Office of Environment, Safety and Health
Office of Environmental Management
Office of Fossil Energy
Office of General Counsel
Office of Health, Safety, and Security
Office of Hearings and Appeals
Office of Human Capital Management
Office of the Inspector General
Office of Intelligence and Counterintelligence
Office of Legacy Management
Office of Management
National Nuclear Security Administration
Office of Nuclear Energy
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

ATTACHMENT 2

DEFINITIONS

Alert—A time-critical message or posting to notify DOE organizations that they are in imminent danger of attack. The designation “alert” is used for notifications about attacks at other DOE sites, Federal agencies, or organizations.

Normal Business Hours—Hours during which normal DOE business is conducted.

Compromise—Incident resulting in the loss of data, data integrity, data confidentiality, and/or system control to any network resource (PC, router, server, firewall, etc.).

Critical Infrastructure Protection (CIP) Asset—Infrastructure resources listed in an Agency’s CIP inventory under Project Matrix.

Cyber Security Incident—Any adverse event that threatens the security of information resources, including loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability.

Denial of Service—Type of incident resulting from any action or series of actions that prevents any part of an IS from functioning.

DOE Contractor—Entity that receives an award from DOE, including management and operating contractors who manage, operate, or provide Primary DOE Organization services to DOE research or production facilities that are principally engaged in work for DOE.

Heads-Up Notice and/or Bulletin—A routine message identifying vulnerabilities and recommended fixes.

Incident Type—Occurrence that has been assessed as having an adverse effect on the security or performance of a system. A single measured cyber-attack. (The problem with “incidents” is that it is often hard to quantify exactly what is going on. Sometimes incidents are detected that are actually due to networking anomalies that have nothing to do with hacking. Therefore, an incident starts life when something is detected. As time goes on, the incident will be updated with more information, such as grouping together related attacks.)

Information System—Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information.

Intrusion Detection—Logging and auditing capability that provides evidence that an attempted or actual breach of protection mechanisms or access controls has occurred.

Malicious Code—Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system.

Need-To-Know. A determination made by an authorized holder of classified or unclassified information that a prospective recipient requires access to specific classified or unclassified information in order to perform or assist in a lawful and authorized Governmental function.

Nonrepudiation—Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity so neither can later deny having processed the data.

Persistent Incident—Consistent and continual attack on an asset that is determined by the Primary DOE Organization or subordinate organization, in accordance with its governing Program Cyber Security Plan, to be above the daily noise level and deserving of attention (that is, because something makes the incident stand out from other activity as something that requires attention or investigation).

Security-Significant Change. A change in an accredited system, its environment, protection requirements, threats, or the implementation of protection requirements which alters the risk to the system sufficiently that re-accreditation of the system is required.

Significant Incident. Detected activity that deviates from the expected behavior of users of the system that is different from known signature attacks or an activity that stands out from the daily noise level and that the Primary DOE Organization or subordinate organization determines, in accordance with its governing Program Cyber Security Plan, to require attention or investigation.

Unauthorized Disclosure. A communication or physical transfer of classified or unclassified matter and/or information to an unauthorized recipient.

Web Site Defacement. An incident resulting in the loss of data or data integrity to a Web server that could result in misinformation to DOE customers and collaboration partners, DOE embarrassment, or the total loss of service.