MANUAL

DOE M 205.1-8

Approved: 1-8-09
Admin Chg 1: 9-1-09
Admin Chg 2: 12-22-09

CYBER SECURITY INCIDENT MANAGEMENT MANUAL

U.S. DEPARTMENT OF ENERGY
Office of the Chief Information Officer

AVAILABLE ONLINE AT:
www.directives.doe.gov

INITIATED BY:
Office of the Chief Information Officer

CYBER SECURITY INCIDENT MANAGEMENT MANUAL

1. PURPOSE. This Department of Energy (DOE) Manual establishes the minimum requirements for a structured cyber security incident management process for identifying, categorizing, containing, reporting, and mitigating cyber security incidents involving DOE information and information systems operated by DOE or by contractors on behalf of the Department.

2. CANCELLATIONS. None.

3. APPLICABILITY.

   a. All Departmental Elements. Except for the exclusions in paragraph 3c, this Manual applies to Departmental elements that utilize information systems to collect, process, store, display, create, disseminate, or transmit national security or unclassified DOE information, hereafter called DOE information systems. (Go to www.directives.doe.gov/pdfs/reftools/org-list.pdf for the current listing of Departmental elements).

      The Administrator of the National Nuclear Security Administration (NNSA) will assure that NNSA employees and contractors comply with their respective responsibilities under this Manual. Nothing in this Manual will be construed to interfere with the NNSA Administrator's authority under section 3212(d) of Public Law (P.L.) 106-65 to establish Administration specific policies, unless disapproved by the Secretary.

   b. DOE Contractors.

      (1) Except for the exclusions in paragraph 3c, the Contractor Requirements Document (CRD), Attachment 1, sets forth requirements of this Manual that will apply to site/facility management contracts that include the CRD.

      (2) This CRD will be included in all contracts that involve information systems that are used or operated by a contractor or other organization on behalf of DOE, including NNSA, to collect, process, store, display, create, disseminate, or transmit national security or unclassified DOE/ government information.

      (3) This Manual does not automatically apply to other than site/facility management contracts. Application of any of the requirements of this Manual to other than site/facility management contracts (e.g., contracts that involve Information Systems processing DOE information and contain

DEAR clause 952.204-2, *Security requirements*) will be communicated as appropriate through heads of field elements, heads of Headquarters Departmental elements, or contracting officers.

c. Exclusions.

(1) In accordance with the responsibilities and authorities assigned by Executive Order (E.O.) 12344, codified at 50 USC sections 2406 and 2511 and to ensure consistency throughout the joint Navy/DOE Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors (Director) will implement and oversee requirements and practices pertaining to this Manual for activities under the Director's cognizance, as deemed appropriate.

(2) Information systems designated as intelligence systems are subject to the requirements of the Director of National Intelligence Directives and Intelligence Community Directives and are thereafter excluded from the requirements of this Manual.

4. REQUIREMENTS. This Manual establishes the minimum cyber security incident management requirements, including processes for identifying incidents and managing the reporting and mitigation of incidents after they have been identified, including assignment of responsibilities. These requirements must be followed in the management and operation of all unclassified and National Security System (NSS) information systems operated by and on behalf of DOE.

a. The requirements of this Manual are in addition to those outlined in DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, and do not relieve any organization from the requirements therein.

b. The requirements of this Manual are in addition to those outlined in DOE O 475.1, *Counterintelligence Program*, and do not relieve any organization from the requirements therein; the DOE Cyber Incident Response Capability (DOE-CIRC) reports on all applicable cyber security incidents per the requirements of DOE O 475.1 on behalf of all Departmental Elements.

c. Cyber security incidents involving national security information systems must be reported in accordance with the requirements in DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, and then reported to DOE-CIRC after the reporting required by DOE M 470.4-1 is completed. The DOE-CIRC report must be unclassified and contain sufficient information to allow DOE-CIRC to access the report submitted under DOE M 470.1-4.

d. Senior DOE Management, as defined in DOE O 205.1A, *Department of Energy Cyber Security Management*, dated 12-4-06, may add to these requirements for

their own organizations, based on assessment of risk, so long as any additional direction is consistent with these requirements.

e. Senior DOE Management Program Cyber Security Plans (PCSPs) must require their operating units to implement and maintain at least the minimum requirements in this Manual for information systems operated by or on behalf of the Department no later than 6-30-2010. If an operating unit cannot implement the requirements of this Manual by the scheduled milestone, the operating unit must establish a plan of action and milestones (POA&M) for implementation of the requirements.

5. RESPONSIBILITIES.

a. The DOE-CIRC is responsible for Department-wide management of cyber security incidents, including reporting, consolidation, correlation, and management functions. The DOE-CIRC is jointly overseen by OCIO and NNSA.

b. The head of the Departmental element is responsible for ensuring that the CRD at Attachment 1 is included in all contracts that involve information systems used or operated by a contractor or other organization on behalf of DOE, including NNSA, to collect, process, store, display, create, disseminate, or transmit national security or unclassified DOE/ Government information. Once notified, the contracting officer is responsible for incorporating the CRD into each affected contract.

6. REFERENCES.

a. Executive Orders.

(1) E.O. 13010, *Critical Infrastructure Protection*, as amended, dated July 15, 1996.

(2) E.O. 13011, *Federal Information Technology*, dated July 16, 1996.

(3) E.O. 13231, *Critical Infrastructure Protection in the Information Age*, dated October 16, 2001.

b. Homeland Security Presidential Directives. HSPDs are available online at http://www.dhs.gov/xabout/laws/editorial_0607.shtm.

Homeland Security Presidential Directive (HSPD)-7, *Critical Infrastructure Identification, Prioritization, and Protection*, dated December 17, 2003.

c. Office of Management and Budget (OMB). Circulars are available online at http://www.whitehouse.gov/OMB/circulars/index.html.

Vertical line denotes change.

(1) OMB Circular A-130, *Management of Federal Information Resources*, November 2000.

(2) OMB Memorandum (M) 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007.

(3) OMB M-07-19, *FY2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, July 25, 2007.

(4) OMB M-06-16, *Recommendations for Identity Theft Related Data and Breach Notification,* September 20, 2006.

(5) OMB M-06-19, *Reporting Incidents Involving Personally Identifiable Information Incorporating the Cost for Security in Agency Information Technology Investments*, July 12, 2006.

(6) OMB M-06-15, *Safeguarding Personally Identifiable Information*, May 22, 2006.

(7) OMB Memorandum M-04-15, *Development of Homeland Security Presidential Directive (HSPD) – 7 Critical Infrastructure Protection Plans to Protect Federal Critical Infrastructures and Key Resources*, June 17, 2004.

d. National Security.

(1) National Security Directive (NSD) 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, dated 7-5-90 (online at http://www.fas.org/irp/offdocs/nsd/nsd_42.htm).

(2) National Security Telecommunications and Information Systems Security Advisory Memorandum INFOSEC 1-99, *The Insider Threat to U. S. Government Information Systems*, dated July 1999 (online at http://www.cnss.gov/Assets/pdf/nstissam_infosec_1-99.pdf).

(3) National Security Telecommunications and Information System Security Instruction No. 1000, *National Information Assurance Certification and Accreditation Process*, dated April 2000 (online at http://www.cnss.gov/Assets/pdf/nstissi_1000.pdf).

e. National Institute of Standards and Technology (NIST) Special Publications. Find NIST Special Publications at http://csrc.nist.gov/publications/PubsSPs.html.

(1) NIST Special Publication (NIST SP) 800-61 Revision 1, *Computer Security Incident Handling Guide*, dated March 2008.

(2) NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*, dated November 2005.

(3) NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, dated August 2006.

f. DOE Directives. Find directives online at www.directives.doe.gov.

(1) DOE O 142.3, *Unclassified Foreign Visits and Assignments Program*, dated 6-18-04.

(2) DOE M 205.1-3, *Telecommunications Security Manual*, dated 4-17-06.

(3) DOE M 205.1-4, *National Security System Manual*, dated 3-8-07.

(4) DOE M 205.1-5, *Cyber Security Process Requirements Manual*, dated 8-12-08.

(5) DOE P 205.1, *Departmental Cyber Security Management Policy*, dated 5-8-01.

(6) DOE O 205.1A, *Department of Energy Cyber Security Management*, dated 12-4-06.

(7) DOE N 221.14, *Reporting Fraud, Waste, and Abuse*, dated 12-20-07

(8) DOE O 221.1A, *Reporting Fraud, Waste, and Abuse to the Office of Inspector General*, dated 4-19-08.

(9) DOE O 221.2A, *Cooperation with the Office of Inspector General*, dated 2-25-08.

(10) DOE O 226.1A, *Implementation of Department of Energy Oversight Policy*, dated 7-31-07.

(11) DOE P 470.1, *Integrated Safeguards and Security Management (ISSM) Policy*, dated 5-8-01.

(12) DOE O 470.2B, *Independent Oversight and Performance Assurance Program*, dated 10-31-02.

(13) DOE O 470.4A, *Safeguards and Security Program*, dated 5-25-07.

(14) DOE M 470.4-1 Chg 1, *Safeguards and Security Program Planning and Management*, dated 8-26-05.

(15) DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information*, dated 6-30-00.

(16) DOE O 471.3, *Identifying and Protecting Official Use Only Information*, dated 4-9-03.

(17) DOE O 475.1, *Counterintelligence Program*, dated 12-10-04.

(18) DOE O 475.2, *Identifying Classified Information*, dated 8-28-07.

g. Other.

(1) E-Government Act of 2002 (P.L. 107-347), December 17, 2002.

(2) Title XXXII of P.L. 106-65, National Nuclear Security Administration Act, as amended, which established a separately organized agency within the Department of Energy.

(3) Title 44, United States Code, Chapter 35, Subchapter III, § 3547. National Security Systems.

(4) Clinger-Cohen Act of 1996, P.L 104-106, Divisions D and E, 110 Stat. 186 (codified as amended in scattered sections of 40 and 41 U.S.C.).

(5) Atomic Energy Act of 1954, as amended (codified at 42 U.S.C. §§ 2011-2286i, 2297f-2297g-4).

7. DEFINITIONS.

a. DOE Cyber Emergency Condition. A DOE-wide comprehensive cyber defense posture and response based on the status of information systems, incident management activities, and intelligence assessments. In emergency conditions, DOE-wide actions are required to defend and mitigate against computer network attacks and to mitigate sustained damage to the DOE information infrastructure.

b. DOE-CIRC Alerts. Communication from DOE-CIRC regarding imminent issues that could affect or is affecting the Department's or an Operating Unit's security operations and posture (e.g., when the DOE and sites are under widespread attack, if mission-critical departmental resources are at great risk of compromise, etc.). Operating Unit actions in response to the Alert are not mandatory

c. Information System (IS). A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, transmission, disposition, or dissemination of information [Source: NIST SP 800-53; FIPS 200; FIPS 199; 44 U.S.C. Sec. 3502; OMB Circular A-130, App. III]. NOTE: Information systems include personnel, hardware, software, and procedures that support the operation of the system. An information system may be a general support system

or major application and include specialized systems such as industrial/process control systems, telephone switching/private branch exchange (PBX) systems, and environmental control systems.

d. Operating Unit. A subordinate element, such as a program office, field office, or contractor, reporting to an Under Secretary, the Department of Energy Chief Information Officer, the Power Marketing Administrations, or heads of Departmental elements.

e. Senior DOE Management. For the purposes of this Manual, the Under Secretaries, the NNSA Administrator, Energy Information Administration, Power Marketing Administrations, and the Chief Information Officer.

8. CONTACT. Questions concerning this Manual should be addressed to the Office of the Chief Information Officer at 202-586-0166.

BY ORDER OF THE SECRETARY OF ENERGY:

JEFFREY F. KUPFER
Acting Deputy Secretary

CONTENTS

.

CHAPTER I. REQUIREMENTS

1. INCIDENT MANAGEMENT. This Manual establishes the framework for the DOE incident detection, warning, and response capability for national security and unclassified cyber systems. It defines, within DOE, the roles, responsibilities, and required processes for Department-wide proactive analysis of individual incidents and DOE-wide incidents, and corrective actions to mitigate or reduce the occurrence of cyber security incidents.

   a. Senior DOE Management must address in their PCSPs cyber security incident management requirements for their operating units, including the minimum requirements of this Manual and any organization-specific incident management policies and procedures. At a minimum, the PCSP must address the requirements of this Manual and define the Senior DOE Management structure and processes for incident handling, reporting, mitigation, impact assessment, and responding to DOE-wide cyber security incident-related alerts and DOE Cyber Emergency declarations.

   b. Each Operating Unit must develop and maintain a Cyber Incident Response Management Plan that details the operating unit's incident management policies and procedures. At a minimum, the plan must address the following.

      (1) Incident management organization for incident handling and reporting, including a Cyber Incident Response Team (CIRT) point of contact, CIRT members, local experts, and the roles and responsibilities of cyber security incident management personnel. CIRT staff must be available for contact (on-call or on-site) 24 hours a day, 7 days per week.

      (2) Cyber security incident mitigation strategies.

      (3) Processes, policies, and procedures for detection and analysis, containment, eradication, recovery and reporting of cyber security incidents to the DOE-CIRC and management, as required by the PCSP

      (4) Processes and procedures for restricting access, testing, or touching, at DOE-CIRC direction, of any cyber resource identified as part of any on-going cyber security incident or investigation, aside from automated filtering or computer network defense devices for network defense.

      (5) The Operating Unit's processes and procedures for assessing and responding to DOE-CIRC Alerts.

      (6) The Operating Unit's processes and procedures for responding to DOE Cyber Emergency conditions. Processes and procedures for responding to DOE Cyber Emergency declarations must include—

(a) performing DOE Cyber Emergency actions requested by DOE-CIRC,

(b) integrating response measures with Operating Unit Security Condition (SECON) procedures, emergency procedures, Continuity of Operations (COOP), and incident handling procedures,

(c) testing and reviewing, response measures and reporting procedures annually and updating as needed,

(d) operational impact assessments to identify all information systems and applications required to maintain the operating unit's primary missions, and

(e) procedures for rapid reconfiguration, as needed, of mission critical systems and applications to ensure appropriate level of protection to those services and systems.

(7) Categorization and impact assessments.

(8) Incident handling and reporting, including incidents involving Personally Identifiable Information (PII). Polices established by the Senior Agency Official for Privacy (SAOP) contain the definition of PII

(9) Maintenance of incident records.

2. EQUIVALENCIES AND EXEMPTIONS. Requests for equivalencies and exemptions from the requirements of this Manual must be supported with a risk assessment that identifies the risks to be accepted.

a. Equivalencies. Equivalencies are approved conditions that technically differ from a requirement in this Manual but afford designated approving authority (DAA)-approved equivalent levels of protection either with or without compensatory measures.

(1) Equivalency requests must be submitted in writing to the cognizant DAA and include detailed description of the requirements and rationale for the equivalency. The equivalency documentation must be included or referenced in the system security plan (SSP).

(2) The cognizant DAA will review and approve or disapprove the equivalency with comments and recommendations in writing.

(3) Equivalencies will be approved for no longer than 3 years, can be extended through request resubmission and must be documented or referenced in the SSP.

b. Exemptions. Exemptions are approved deviations from a requirement in this Manual that may create a security vulnerability. Exemptions will be approved only when correction of the condition is not feasible or cost effective.

(1) Requests for exemptions and supporting documentation must be submitted in writing by the DAA to the cognizant Senior DOE Manager for review and approval. Documentation supporting the exemption request and DAA's acceptance of associated residual risk must identify the requirements that cannot be met, compensatory measures implemented, and compensatory measures.

(2) Cognizant Senior DOE Management must review and approve/disapprove the exemption request and provide a final written decision to the DAA. A copy of the approved exception must be provided to the DOE CIO.

(3) Approved exemptions will remain in effect no longer than 3 years and must be documented or referenced in the SSP.

3. INCIDENT CATEGORIZATION AND IMPACT ASSESSMENT. Senior DOE Management PCSPs must require operating units to document incident management processes, policies, and procedures to categorize, assess, and mitigate incident impact in accordance to requirements of this Manual and the applicable PCSP.

a. Identified cyber security incidents must be categorized according to potential negative impact to information and/or information systems. This categorization is based on two assigned criteria: Incident Type and Incident Category, as described below.

b. Incident Types. Cyber security incidents are classified as either Type 1 or Type 2 as described below depending upon the type of security violation.

(1) Type 1 incidents are successful incidents that potentially create serious breaches of DOE cyber security. The following are defined as Type 1 incidents.

(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 information technology resources, including media that contains Sensitive Unclassified Information (SUI), PII 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.

(f) Critical Infrastructure Protection (CIP). Any unplanned activity that adversely affects an asset identified as critical infrastructure.

(g) Unauthorized Use. Any activity that adversely affects an information system's normal, baseline performance and/or is not recognized as being related to an Operating Unit or Senior DOE Management mission. Unauthorized use includes, but is not limited to, port scanning that excessively degrades performance; IP (Internet protocol) spoofing; network reconnaissance; monitoring; compromised DOE servers; or illegal activities.

(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 (e.g., classified on an unclassified network, SUI/PII transmitted via the Internet unencrypted, 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 that stands out above the daily activity or noise level and could result in unauthorized access (compromise) if the system were not protected.

(b) Reconnaissance Activity. Persistent surveillance and resource mapping probes and scans 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 parameters for collecting and reporting data on surveillance probes and scans must be documented.

c. Incident Categories. An impact assessment for each cyber security incident must be conducted by the Operating Unit to determine the incident category as described below.

(1) Cyber security incidents are categorized based on an assessment of potential impact to the confidentiality, integrity, and/or availability of DOE information or an information system and the resulting adverse effect on DOE operations, assets, mission, or reputation.

(a) 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 (other than a PII breach), including loss of secondary mission capability, requiring minor corrective actions or repairs.

(b) 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.

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

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

(2) Incidents involving PII are categorized either moderate or high depending on the severity of the breach.

4. INCIDENT HANDLING AND REPORTING. Senior DOE Management PCSPs must require operating units to act as follows when a cyber security incident has occurred or is suspected to have occurred (i.e., potential incident).

   a. Immediately examine and document the pertinent facts and circumstances surrounding the event.

   b. Report the pertinent facts and circumstances surrounding a suspected/potential incident to DOE-CIRC in accordance with the timeframes in Table 1. This initial report should include as many of the following as possible at the time of the initial report.

      (1) name of organization;

      (2) contact information for incident (name, telephone, email address);

      (3) physical location of affected computer/network;

      (4) type of information the compromised system was accredited to process (e.g., Classified, Unclassified, OUO, etc.);

      (5) date incident occurred;

      (6) time incident occurred (include time zone);

      (7) type and impact category of incident (e.g., intrusion/moderate impact, denial of service/high impact, etc.);

      (8) internet protocol (IP) address and domain name of affected system(s) (destination IP, port, protocol);

      (9) IP address and domain name of apparent attacker if known (source IP, port, protocol);

      (10) suspected method of intrusion/attack;

      (11) suspected perpetrators and/or possible motivations;

   c. Complete the initial investigation of an event within 24 hours. If the initial investigation of an event 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. If a security breach of PII has occurred, reporting must be completed in accordance with the requirements defined by the SAOP.

d. Upon confirmation of an incident, categorize and report to DOE-CIRC in accordance with the time frames indicated in Table 1.

Table 1: Reporting Time Frames

Incident Type	Incident Category					
	Low	Moderate		High		Very High
Suspected/Potential Type 1[1]	Within 4 hours	Within 2 hours	PII* within 45 minutes	Within 1 hour	PII* within 45 minutes	Within 1 hour
All Type 2 and Confirmed Type 1	Within 1 week	Within 48 hours		Within 24 hours		Within 8 hours

*PII is Personally Identifiable Information. Refer to SAOP requirements documents for the definition of PII.

e. Prepare and retain documentation for all incident evaluations and incidents. At a minimum, the following information is to be included if applicable[2]. Not all information will apply to every incident.

(1) name of organization;

(2) contact information for incident (name, telephone, email address);

(3) physical location of affected computer/network;

(4) type of information the compromised system was accredited to process (e.g., Classified, Unclassified, OUO, etc.);

(5) date incident occurred;

(6) time incident occurred (include time zone);

(7) description of affected critical infrastructure if applicable;

(8) type and impact category of incident (e.g., intrusion/moderate impact, denial of service/high impact, etc.);

(9) internet protocol (IP) address and domain name of affected system(s) (destination IP, port, protocol);

---

[1] All Type 1 incidents must be reported.

[2] The type and volume of information maintained regarding an incident may be classified and should be protected accordingly.

(10) IP address and domain name of apparent attacker if known (source IP, port, protocol);

(11) operating system of affected host(s) (version, patch-level);

(12) functions of affected host(s);

(13) number of affected host(s);

(14) suspected method of intrusion/attack;

(15) suspected perpetrators and/or possible motivations;

(16) evidence of spoofing;

(17) application software affected;

(18) description of security infrastructure in place at time of incident;

(19) whether the intrusion resulted in a loss or modification of DOE information;

(20) if PII was involved, have affected organizations/individuals been notified;

(21) evidence of damage to the affected system(s) to include level of unauthorized access;

(22) description of hacking tools and/or techniques used if applicable;

(23) what vulnerability was exploited, if applicable;

(24) description of investigation actions and mitigation efforts;

(25) last time the affected system(s) were modified or powered up;

(26) assessment of incident impact;

(27) anti virus installed, included version and latest updates; and

(28) method of identifying the incident (e.g., IDS, audit log analysis, system administrators, etc.).

f. Organizations that do not have successful or attempted incidents during the reporting period must submit a report of no activity to the DOE-CIRC. (Automated systems may be used for reporting if reporting by such systems complies with Senior DOE Management requirements.).

5. CYBER SECURITY ALERTS AND CYBER EMERGENCIES. Senior DOE Management PCSPs must require operating units to develop, document, and implement procedures for handling information disseminated by the DOE-CIRC, responding proactively to alerts and DOE Cyber Emergency declarations, analyzing threat information, and performing corrective/ preventive actions as required. At a minimum, these procedures must include—

   a. Acknowledging to the DOE-CIRC receipt of an Alert or a DOE Cyber Emergency declaration by the Operating Unit within 4 business hours;

   b. Executing analyses relative to the activities described in the alert or DOE Cyber Emergency declaration;

   c. Executing appropriate corrective/ preventive actions; and

   d. Reporting to the DOE-CIRC the actions taken or provide justification for actions not taken.

CHAPTER II. RESPONSIBILITIES

Senior DOE Management is responsible for ensuring the implementation of the DOE Cyber Security Program, this Manual, and any Senior DOE Management identified additional requirements.

1. SENIOR DOE MANAGEMENT.

   a. Ensure the implementation of this Manual by the Operating Units under their purview for all information systems that collect, process, store, display, create, disseminate, or transmit information by or on behalf of the Department through the PCSP.

   b. Determine the need for and develop any additional requirements to this Manual for the Operating Units under their purview and ensure that the Operating Units implement those requirements.

   c. Ensure the Contracting Officers are notified to incorporate the CRD into affected contracts.

   d. Ensure the coordination of incident management activities for incidents that span multiple Operating Units under their purview.

   e. Ensure that each Operating Units develops a Cyber Incident Response Management Plan, which includes roles and responsibilities for incident and DOE-CIRC alert response or DOE Cyber Emergency declaration, and a formalized set of procedures for handling, reporting to DOE-CIRC, and monitoring for information technology security incidents.

   f. Ensure that incidents are reported to the DOE-CIRC within reporting time requirements.

   g. Ensure that Operating Unit response measures are developed for DOE Cyber Emergency declarations and copies are furnished to the DOE-CIRC.

   h. Ensure that each Operating Unit implements their documented processes and procedures in response to a DOE Cyber Emergency declaration.

   i. Ensure the integration of DOE Cyber Emergency declaration response measures with Operating Unit Security Condition (SECON) procedures, emergency procedures, Continuity of Operations plans, and incident handling procedures.

   j. Ensure that DOE Cyber Emergency response measures and reporting procedures are tested and reviewed at least annually, and updated as needed..

k. Ensure a process is established, documented, tested, and included in the PCSP for subordinate organizations to report all cyber security incidents to:

(1) DOE-CIRC and, where appropriate, in coordination with the DOE-CIRC, to law enforcement authorities (e.g., Inspector General, Federal Bureau of Investigation, local police, etc.).

(2) Senior DOE Management and the Senior Management of the Operating Unit and/or the investigating organizations, as appropriate.

l. Ensure that each Operating Unit works with the DOE-CIRC on the handling, reporting, and mitigation of cyber security incidents.

m. Ensure Operating Units cooperate with the Office of Inspector General

2. DOE CHIEF INFORMATION OFFICER. In addition to his/her responsibilities as a Senior DOE Manager as described in paragraph 1 above, the DOE CIO—

a. Performs an annual review of this Manual and update as necessary.

b. Ensures the availability of Departmental Incident Management assistance through the DOE-CIRC for monitoring, reporting, and coordination of incidents within the Department.

c. Ensures the coordination of incident management/response activities for incidents that span Senior DOE Management Organizations.

d. Coordinates reporting to and interaction with OMB, the Federal CIO Council, and other Federal policy officials concerning threats, vulnerabilities, and incidents of Government-wide significance in consultation with the reporting entity.

e. Jointly oversees the DOE-CIRC with NNSA.

f. Ensures the dissemination of information on cyber security incidents, as appropriate, to US-CERT, DOE-CIRC, Senior DOE Management, and Department-level senior management in consultation with the reporting entity.

g. Ensures reporting and coordination of incidents involving Personally Identifiable Information with the Senior Agency Official for Privacy in consultation with the reporting entity.

h. Coordinates with the reporting entity all public release of cyber security incident information.

i. Ensures issuance of DOE Cyber Emergency declarations through the DOE-CIRC.

j. Ensures reporting and coordination of Type 1 incidents in a timely manner with the Office of Inspector General.

3. CONTRACTING OFFICER.

a. Once notified of contractor applicability, incorporates the CRD into affected contracts.

b. Assists in incorporating the CRD in new contracts when notified of the applicability.

APPENDIX A
DOE CYBER EMERGENCY DECLARATIONS

1. DOE Cyber Emergency. A DOE-wide cyber defense response based on the status of information systems, incident management activities, and intelligence assessments, especially when DOE-wide actions are required to defend against computer network attacks and to mitigate wide-spread damage to the DOE information infrastructure.

2. DOE Cyber Emergency Determination. There are broad categories of factors that influence a DOE Cyber Emergency declaration: operational, technical, and intelligence, including foreign intelligence and law enforcement intelligence. The DOE Cyber Emergency declaration is based on significant changes in one or more of these factors. The following are some of the factors used to assess the need for a DOE Cyber Emergency declaration. Changes in one or more of these factors may signal a computer network attack (CNA) or computer network exploit (CNE) and may require a DOE Cyber Emergency declaration:

   a. Indications and warnings (including domestic threats): National Security Agency (NSA) Alerts; National Infrastructure Protection Center (NIPC) advisories, US-CERT advisories, threats, warnings; law enforcement agency intrusion reports, etc.

   b. CNA/CNE intelligence assessments

   c. Current world situation

   d. Other alert systems, such as Security Condition (SECON), etc.

   e. System criticality and readiness

   f. Status of coordination for protection of Critical Infrastructure and Key Resources identified under Homeland Security Presidential Directive-7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection*

   g. Incident reports

   h. Trend analyses

CONTRACTOR REQUIREMENTS DOCUMENT

DOE M 205.1-8, *Cyber Security Incident Management Manual*

This Contractor Requirements Document (CRD) establishes the requirements for Department of Energy (DOE) contractors whose contracts involve information systems that collect, process, store, display, create, disseminate, or transmit national security or unclassified DOE/ Government information.

Regardless of the performer of the work, the contractor is responsible for implementing and complying with the requirements of this CRD and the applicable Senior DOE Management Program Cyber Security Plan (PCSP).

The contractor is responsible for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's compliance with the requirements.

Contractor managers or system owners may specify and implement additional requirements to address specific risks, vulnerabilities, or threats within its operating unit/ systems.

U.S. Department of Energy
Washington, D.C.

ADMIN CHANGE

DOE M 205.1-8 Chg 1

Approved: 1-8-09
Admin Chg 1: 9-1-09

SUBJECT: CYBER SECURITY INCIDENT MANAGEMENT MANUAL

1. PURPOSE. To transmit the revised page to DOE M 205.1-8, *Cyber Security Incident Management Manual,* dated 1-8-09.

2. EXPLANATION OF CHANGES. This change amends the date for Senior DOE Management Program Security Plans to require their operating units to implement and maintain at least the minimum requirements of the Manual for information systems operated by or on behalf of the Department.

3. LOCATION OF CHANGE.

Page	Paragraph
iii	4.e.

After filing the attached pages, this transmittal may be discarded.

BY ORDER OF THE SECRETARY OF ENERGY:

KEVIN T. HAGERTY
Director
Office of Information Resources
Office of Management

U.S. Department of Energy
Washington, D.C.

ADMIN CHANGE

DOE M 205.1-8 Chg 2

Approved: 1-8-09
Admin Chg 1: 9-1-09
Admin Chg 2: 12-22-09

SUBJECT: CYBER SECURITY INCIDENT MANAGEMENT MANUAL

1. PURPOSE. To transmit the revised page to DOE M 205.1-8, *Cyber Security Incident Management Manual,* dated 1-8-09.

2. EXPLANATION OF CHANGES. This change amends the date to facilitate the orderly transition to an improved Departmental cyber security governance structure following the cyber security management direction memorandum signed by the Deputy Secretary on December 7, 2009.

3. LOCATION OF CHANGE.

Page	Paragraph
iii	4.e.

After filing the attached pages, this transmittal may be discarded.

BY ORDER OF THE SECRETARY OF ENERGY:

KEVIN T. HAGERTY
Director
Office of Information Resources
Office of Management