DOE M 205.1-1

Approved: 9-30-04
Review: 9-30-06
Expires: 9-30-08

INCIDENT PREVENTION, WARNING, AND RESPONSE (IPWAR) MANUAL

U.S. DEPARTMENT OF ENERGY

Office of the Chief Information Officer

AVAILABLE ONLINE AT:
http://www.directives.doe.gov

INITIATED BY:
Office of the Chief Information Officer

INCIDENT PREVENTION, WARNING, AND RESPONSE (IPWAR) MANUAL

1. OBJECTIVES.

   a. To define a structured, cohesive, and consistent process for performing incident prevention, warning, and response (sometimes referred to collectively as incident handling) for the Department of Energy's (DOE) Federal information systems, which include national security systems, as defined in accordance with Federal law and information security policy and guidance. Except where noted, requirements for Federal information systems also will apply to national security systems.

   b. To provide requirements and implementation instructions for DOE's IPWAR process to supplement DOE O 205.1, *Department of Energy Cyber Security Management Program,* dated 3-21-03.

   c. To assist the Department and Primary DOE Organizations in—

      (1) preparing for, preventing, warning of, and recovering from cyber security incidents through the timely sharing of information regarding vulnerabilities, threats, attempted and successful exploits, and other anomalous activities;

      (2) identifying the roles and responsibilities necessary to promote an effective Department-wide IPWAR capability;

      (3) developing appropriate local IPWAR procedures;

      (4) standardizing reporting procedures to improve timeliness, increase clarity, support effective analysis, and ensure consistency with and provide necessary support to Government-wide requirements and capabilities; and

      (5) measuring the performance of DOE IPWAR capabilities to promote a process of continuing improvement.

   d. To ensure the Department meets the requirements of Federal laws, Executive orders, national security directives, and other regulations.

2. CANCELLATIONS. DOE N 205.4, *Handling Cyber Security Alerts and Advisories and Reporting Cyber Security Incidents,* dated 3-18-02. Cancellation of a DOE Directive does not, by itself, modify or otherwise affect any contractual obligation to comply with the Directive. Cancelled Directives that are incorporated by reference in a contract remain in effect until the contract is modified to delete the references to the requirements in the cancelled Directives.

3. APPLICABILITY.

a. Primary DOE Organizations, Including National Nuclear Security Administration (NNSA) Organizations. Except for the exclusions in paragraph 3c, this Manual applies to any of those Primary DOE Organizations that own or operate Federal information systems (See Attachment 1 for a complete list of Primary DOE Organizations).

The Administrator of NNSA will ensure that NNSA employees and contractors comply with the requirements of this Manual.

b. Site/Facility Management Contractors.

(1) Except for the exclusions in paragraph 3c, the Contractor Requirements Document (CRD), Attachment 2, sets forth the requirements of this Manual that will apply to those site/facility management contractors whose contracts include the CRD.

(2) The CRD must be included in all site/facility management contracts that require or involve access to DOE information systems.

(3) This CRD does not automatically apply to other than site/facility management contractors. Any application of any requirements of this Manual to other than site/facility management contractors will be communicated separately from this Manual.

(4) The heads of Primary DOE Organizations are responsible for notifying contracting officers of which site/facility management contractors are affected by this Manual (see Attachment 3). Once notified, contracting officers are responsible for incorporating the CRD into each affected site/facility management contract via the laws, regulations, and DOE Directives clause of the contract.

(5) As the laws, regulations, and DOE Directives clause of site/facility management contracts states, regardless of who performs the work, site/facility management contractors with a CRD incorporated into their contracts are responsible for complying with the requirements of the CRD.

(a) Affected site/facility management contractors are responsible for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the site/facility management contractors' compliance with the requirements.

(b) Affected site/facility management contractors must not unnecessarily or imprudently flow down requirements to subcontractors. That is, affected contractors will—

1 ensure that they and their subcontractors comply with the requirements of this CRD and

2 only incur costs that would be incurred by a prudent person in the conduct of competitive business.

c. Exclusions. Consistent with the responsibilities identified in Executive Order 12344, the Deputy Administrator for Naval Reactors will ensure consistency throughout 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 Manual for activities under the Deputy Administrator's cognizance.

4. SUMMARY. All Primary DOE Organizations that own, operate, or have access to Federal information systems must report cyber security incidents to the Computer Incident Advisory Capability (CIAC) and other DOE organizations in accordance with the requirements in this Manual. CIAC will then forward the incident information on to the United States Computer Emergency Readiness Team in compliance with Federal legislation and Executive requirements. This document outlines procedures that will improve and measure the performance of the Department's capabilities to prepare for, prevent, warn of, respond to, and recover from cyber incidents.

Chapter I gives background information and outlines requirements. Chapter II lists the responsible officers and their responsibilities. Attachment 1 lists the Primary DOE Organizations to which this Manual applies. Attachment 2 is the CRD. Attachment 3 lists the current contractors to which the Manual's CRD applies. Attachment 4 defines terms pertinent to cyber security and this Manual. Attachment 5 identifies the acronyms used. Attachment 6 is a sample cyber incident response plan. Attachment 7 is a sample incident recognition and reporting worksheet.

5. IMPLEMENTATION. Heads of Primary DOE Organizations must implement the responsibilities and requirements contained in this Manual within 180 days of its issuance. Contractors who provide direct support to Primary DOE Organizations will report through appropriate levels of Primary DOE Organization management.

6. REFERENCES.

a. The following public laws and policies contain cyber security program requirements and guidance that may be helpful in implementing this Manual.

(1) Public Law (P.L.) 107-347, *E-Government Act of 2002,* Title III—Information Security (also known as the *Federal Information Security Management Act of 2002*), December 2002.

(2) Title 18 U.S.C., Section 1030, Fraud and Related Activity in Connection with Computers (also known as the *Computer Fraud and Abuse Act of 1986*).

(3) Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, Appendix III, "Security of Federal Automated Information Resources," November 28, 2000.

(4) OMB Memorandum, "Improved FedCIRC Incident Reporting System," from Mark Forman, OMB Associate Director for Information Technology and Electronic Government, to Chief Information Officers, November 14, 2002.

b. The following national standards and guidelines provide relevant processes and procedures for implementing this Manual.

(1) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, *Computer Security Incident Handling Guide,* January 2004.

(2) NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook,* October 1995.

(3) NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems,* December 1998.

(4) NIST Federal Information Processing Standards Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

c. The following DOE Directives provide relevant requirements and procedures for implementing this Manual.

(1) DOE O 205.1, *Department of Energy Cyber Security Management Program*, dated 3-21-03.

(2) DOE O 221.1, *Reporting Fraud, Waste, and Abuse to the Office of Inspector General,* dated 3-22-01.

(3) DOE 5670.3, *Counterintelligence Program*, dated 9-4-92.

(4) DOE N 221.10, *Reporting Fraud, Waste, and Abuse,* dated 9-15-04.

(5) DOE O 471.4, *Incidents of Security Concern,* dated 3-17-04.

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

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

BY ORDER OF THE SECRETARY OF ENERGY:

KYLE E. McSLARROW
Deputy Secretary

CONTENTS

ATTACHMENTS

CONTENTS (continued)

CHAPTER I. CYBER SECURITY INCIDENT REPORTING REQUIREMENTS

1. INTRODUCTION. The DOE Office of the Associate Chief Information Officer (CIO) for Cyber Security is responsible for Department-wide cyber security policy and for developing supporting guidance. This responsibility was established in DOE O 205.1, *Department of Energy Cyber Security Management Program,* dated 3-21-03. This Manual establishes the framework for the DOE incident prevention, warning, and response (IPWAR) capability for classified and unclassified cyber systems. Its purpose is to define within DOE the roles, responsibilities, and processes for Department-wide proactive analysis and corrective actions to mitigate or reduce the occurrence of cyber security incidents. In addition, the Manual ensures that this aspect of the DOE Cyber Security Management Program meets the requirements of Federal laws, Executive orders, national security directives, and other regulations.

   The Federal Information Security Management Act of 2002 (FISMA) requires Agencies to develop procedures for detecting, reporting, and responding to security incidents, including mitigating risks associated with incidents before substantial damage is done and notifying and consulting with the United States Computer Emergency Readiness Team (US-CERT), law enforcement and inspectors general, and other offices about incidents involving Federal information systems.

   Office of Management and Budget (OMB) policy reminds Agencies of the underlying value of developing and maintaining effective incident detection and reporting programs. Because of the Federal government's inter-networked environment, Agency components that fail to detect and report cyber security incidents will likely cause significant problems throughout the Agency network and may impact other departments and Agencies.[1] Thus the OMB memorandum, *Improved FedCIRC Incident Reporting System* (November 14, 2002), directs agencies to "report all unauthorized system activity (cyber security incidents) quickly and accurately" to the Federal Computer Incident Response Center (FedCIRC, now US-CERT). In addition, in its guidance on fiscal year 2003 reporting under FISMA, OMB directed Agencies to certify in their reports that "both the agency and each of its components have established processes that ensure timely, accurate reporting to US-CERT on security incidents and where appropriate to law enforcement authorities . . . ."

2. REQUIREMENTS.

   a. Categorizing Cyber Security Incidents and Attempted Incidents. Cyber security incidents must be characterized and categorized according to their potential to cause damage to information and information systems based on two criteria: incident type and system impact category.[2] These criteria are used in combination

[1]Memorandum to Chief Information Officers, OMB CIO, "Handling and Reporting Computer Security Incidents," September 12, 2002.

[2]The security categorization of systems established by this Manual is based on National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

to determine the time frame for reporting incidents to the Computer Incident Advisory Capability (CIAC). This Manual establishes two incident types (Type 1 and Type 2) and three categories of system impact (low, moderate, and high), which are described below.

(1) Incident Types.

(a) 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 the currently defined Type 1 incidents (see also Attachment 4, Definitions).

1 *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.

2 *Web Site Defacement*. All instances of a defaced Web site must be reported.

3 *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.

4 *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 by the heads of Primary DOE Organizations.

5 *Critical Infrastructure Protection (CIP)*. Any activity that adversely affects an asset identified as critical infrastructure must be reported. CIP assets are determined by the heads of Primary DOE Organizations.

6 *Unauthorized Use*. Unauthorized use should be construed as any activity that adversely affects an information system's normal, baseline performance and/or is not recognized as being related to DOE's mission. For example, unauthorized use can be using a DOE computer to obtain DOE data without authorization. Unauthorized use can involve using DOE systems to break the law. 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.

(b) 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.

1 *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.

2 *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. Primary DOE Organizations must determine the standard for collecting data on surveillance probes and scans of subordinate sites.

(2) System Impact Categories. System impact 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. System impact 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. Performing this impact analysis is a fundamental step in risk assessment.

Each of the security objectives—confidentiality, integrity, and availability—is assessed in the following manner.

(a) Low Impact. Loss of system confidentiality, integrity, and availability could be expected to have a limited adverse effect on DOE operations, assets, or individuals, requiring minor corrective actions or repairs.

(b) Moderate Impact. Loss of system confidentiality, integrity, and availability could be expected to have a serious adverse effect on

DOE operations, assets, or individuals, including significant degradation or major damage, requiring extensive corrective actions or repairs.

(c) High impact. Loss of system confidentiality, integrity, and availability could be expected to have a severe or catastrophic adverse effect on DOE operations, assets, or individuals. The incident could cause the loss of mission capability for a period that poses a threat to human life or results in the loss of major assets.

b. Reporting Cyber Security Incidents. Departmental incident reporting procedures can be found at the CIAC Web site (www.ciac.org). Requirements for incident reporting must be documented in the Primary DOE Organization's Program Cyber Security Plan (PCSP). Organizations reporting cyber security incidents for national security systems must also follow the requirements outlined in DOE O 471.4, *Incidents of Security Concern*, dated 3-17-04.

(1) Incident Discovery. When a cyber security incident has occurred or is suspected to have occurred, the affected site will immediately examine and document the pertinent facts and circumstances surrounding the incident. (Note: the initial investigation should be completed within 24 hours.)

(2) Incident Reporting and Investigating. Once it is determined that an incident has occurred, the incident must be categorized according to incident type and category of system affected and reported to CIAC within the time frames indicated in Table 1, in accordance with the process established by the Primary DOE Organization.

(3) No Incident. If it is determined that an incident did not occur, no reporting actions are necessary. However, all evaluated and suspected incidents must be documented and local files retained.

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

	System Impact Category		
Incident Type	**Low**	**Moderate**	**High**
Type 1	Within 4 hours[3]	Within 1 hour	Within 1 hour
Type 2	Within 1 week	Within 24 hours	Within 24 hours

[3]Reporting timeframes begin at the point of incident identification.

(4) Monthly Reports. DOE sites must issue a monthly report whether or not it has experienced any reportable successful or attempted cyber security incidents during the previous month. The reporting process must be documented in the Primary DOE Organization's PCSP.

(5) Reporting to the Office of Inspector General. All DOE organizations must inform the Office of Inspector General of all Type 1 incidents consistent with the time frames indicated in Table 1. Reporting this information to the Office of Inspector General must be done according to line of reporting procedures established in the PCSP of the Primary DOE Organization.

(6) Reporting to the Office of Security. All DOE organizations must inform the Office of Security for incidents involving national security systems in accordance with the requirements outlined in DOE O 471.4, *Incidents of Security Concern*, dated 3-17-04.

(7) Reporting to the Office of Counterintelligence. All DOE organizations must inform the Office of Counterintelligence whenever there is suspicion of involvement of a foreign government, entity, or national. Organizations should take appropriate precautions when reporting these incidents and must follow the procedures outlined in DOE O 471.4, *Incidents of Security Concern,* dated 3-17-04, for reporting all incidents involving national security systems.

(8) Automated Systems. Automated systems may be used for reporting if reporting by such systems complies with the requirements of this Manual.

c. Cyber Alerts.

(1) CIAC is the official DOE point of contact for prompt dissemination of information provided in alerts received from external organizations. In addition, CIAC provides DOE responses to national centers, as required. The timing of distribution will be commensurate with the significance of the information.

(2) If CIAC issues an alert, the security points of contact will—

(a) acknowledge the receipt of the alert within 4 normal business hours and

(b) execute the required analyses and appropriate corrective actions and report the actions taken, or provide justification for why actions were not taken, in accordance with the Primary DOE Organization's PCSP.

d. Updating Cyber Security Patches. Security patches must be installed regularly and in a timely manner to help prevent intrusions. The Primary DOE Organization's designated approving authority (DAA) must approve decisions not to apply security patches to systems, as in the case where stability may be sacrificed (and thus availability). All patches and updates must be reviewed for site applicability and 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.

e. Cyber Security Incident Preparedness/Response and Contingency Plans. Because of the interrelationship of cyber security incident preparedness/response and continuity of operations, IPWAR procedures should be integrated into, and tested periodically with the Primary DOE Organizations' information system contingency plans. Contingency plans should include a description of or reference to the IPWAR procedures that would be followed to ensure that the system will continue to have incident protection if a disaster occurs.

f. Cyber Security Incident Training. Primary DOE Organizations must ensure that users, system administrators, and cyber security staff are well-versed in IPWAR procedures through initial and annual refresher computer security awareness training.

CHAPTER II. CYBER SECURITY INCIDENT MANAGEMENT STRUCTURE AND ROLES AND RESPONSIBILITIES

1. INTRODUCTION. To ensure an effective and proactive approach to incident handling, the Department must plan and act across the incident life cycle. This life-cycle-based methodology requires responsible officers/organizations to address their roles and responsibilities before, during, and after an incident has occurred. Therefore, the descriptions of responsibilities in this Manual are presented in the following categories:

   - Prepare and Prevent;
   - Detect, Respond, and Report; and
   - Restore and Improve.

2. OFFICE OF THE CHIEF INFORMATION OFFICER (OCIO).

   a. Prepare and Prevent.

      (1) Maintains emergency contact information for DOE organization cyber security points of contact.

      (2) Provides management and budgetary oversight and guidance to CIAC.

      (3) Provides oversight, coordination, and management for an incident awareness, handling, and training program for all DOE organizations.

      (4) Coordinates and provides overall IPWAR security requirements and definitions.

      (5) Provides standard security banner defining appropriate use of the system for users to view upon login. (This is necessary for establishing criminal culpability.)

   b. Detect, Respond, and Report.

      (1) Establishes organizational approach to incident handling.

      (2) Coordinates reporting to and interaction with OMB, the Federal CIO Council, CIAC, Primary DOE Organizations and other Federal policy officials concerning threats, vulnerabilities, and incidents of Government-wide significance.

      (3) Serves as the primary point of contact and reporting agent on all IPWAR incidents involving the DOE Headquarters site.

c. Restore and Improve.

(1) Measures the performance of and provides overall policy, management, and compliance oversight for the DOE IPWAR capability.

(2) Disseminates information on cyber security incidents, as appropriate, to Department-level senior management, consistent with agreed-on procedures.

(3) Identifies DOE and external IPWAR-related methods, and facilitates the sharing of these methods across DOE.

3. OFFICE OF THE CHIEF INFORMATION OFFICER/COMPUTER INCIDENT ADVISORY CAPABILITY.

a. Prepare and Prevent.

(1) Provides analysis and watch and warning capabilities to prevent cyber security incidents or reduce their impact to the Department.

(2) Correlates data gathered from perimeter scanning with threat and vulnerability alerts to help identify high-risk Primary DOE Organizations.

(3) Provides information to Primary DOE Organizations in a timely manner when security patches for software used by the Department become available.

(4) Provides computer forensics and evidence-handling assistance to individuals investigating and preserving cyber evidence.

(5) Provides incident reporting and information collection aids for use in properly capturing critical information concerning an incident.

b. Detect, Respond, and Report.

(1) Serves as the Department's central cyber incident reporting point of contact for the receipt of alerts, advisories, notices, bulletins, or other cyber security information from external organizations and the receipt of cyber security information from Primary DOE Organizations.

(2) Logs all cyber security incident reports, acknowledges receipt, and assigns incident numbers.

(3) Notifies heads of Primary DOE Organizations in a timely manner, through primary and alternate points of contact, that an alert regarding a threat, vulnerability, and/or associated patch has been posted for their review and action.

(4) Transmits initial reports of cyber security incidents received from Primary DOE Organizations to the DOE Headquarters Emergency Operations Center, and as necessary, transmits subsequent reports to the Associate CIO for Cyber Security and the Office of Security. Consistent with law and policy, reports all cyber security incidents quickly and accurately to US-CERT within the Department of Homeland Security. Where appropriate, reports cyber security incidents to law enforcement authorities in coordination with the affected sites.

(5) In coordination with the lead Primary DOE Organization, assists the Office of the Associate CIO for Cyber Security in determining whether conditions indicate that a multiple-site event that warrants reporting to the Offices of Inspector General, Counterintelligence, and/or Security has occurred or is developing.

(6) Provides incident response assistance to the Department during an active event, including securing and collecting incident information.

c. Restore and Improve.

(1) Provides Primary DOE Organization management with timely and effective technical and nontechnical assistance (tools, methods, and guidance) in response to a cyber security incident.

(2) Provides reports of significant cyber security incidents to the Associate CIO for Cyber Security.

(3) Provides aggregated performance measurement data for the Department to the OCIO on an annual and ad hoc basis.

(4) Collaborates with incident response centers in private industry, the Department of Defense, and other Government agencies.

(5) Provides lessons learned, follow up reports, and recommended updates to security methods to Primary DOE Organizations to improve the Agency's policies and procedures.

4. HEADS OF PRIMARY DOE ORGANIZATIONS.

a. Prepare and Prevent.

(1) Establish, within their respective PCSPs, processes and procedures to ensure that the requirements of this Manual are implemented and documented in their subordinate organizations' Cyber Security Program Plans (CSPPs) or system security plans.

(2) Provide, keep current, and test emergency cyber security point of contact information for Federal and contractor reporting, and ensure that information is provided to the Office of the Associate CIO for Cyber Security.

(3) Ensure that processes to update security software and patches on regular and emergency bases are established and documented in the Primary DOE Organization's PCSP.

(4) Develop a cyber incident response plan, including the scope of the plan, the roles and responsibilities of the Computer Incident Response Team (CIRT), and a formalized set of procedures for reporting and handling cyber security incidents. The computer incident response plan should be included or referenced in the Primary DOE Organization's PCSP document (see Attachment 6 for content of a sample plan).

(5) Ensure CIRTs include representatives from different offices within the Primary DOE Organization who can aid in handling an incident.

(a) Include individuals with competencies matching the roles and responsibilities identified in Attachment 6 of this Manual.

(b) Provide materials and/or train team members on their roles in the incident response process.

(6) Include counterintelligence-related responsibilities in their Primary DOE Organization PCSPs, and ensure compliance with DOE 5670.3, *Counterintelligence Program,* dated 9-4-92, for counterintelligence-related events.

(7) In coordination with the OCIO, establish (and document within their Primary DOE Organization PCSPs) a process for reporting incidents to the Technology Crimes Section of the Office of Inspector General in accordance with DOE O 221.1, *Reporting Fraud, Waste, and Abuse to the Office of Inspector General,* dated 3-22-01; DOE O 471.4, *Incidents of Security Concern,* dated 3-17-04; and DOE N 221.10, *Reporting, Fraud, Waste, and Abuse,* dated 9-15-04.

(8) Ensure that all users, system administrators, and cyber security staff are provided with awareness training, materials, and checklists regarding IPWAR procedures on an initial and annual basis.

b. Detect, Respond, and Report.

(1) Promote incident reporting within the organization and ensure users understand there will be no retaliation for reporting incidents.

(2) Ensure that a process is established, documented, tested, and included in the PCSP for subordinate organizations and DOE sites to report all cyber security incidents (as defined in Chapter I) to CIAC, including negative reporting, and where appropriate, in coordination with the OCIO, to law enforcement authorities.

(3) Establish, within their respective Primary DOE Organization PCSPs, processes and procedures to ensure the requirements of this Manual are implemented and documented in subordinate organization CSPPs, system security plans, and/or Contractor Requirements Documents.

(4) Work with CIAC to determine the severity or significance of cyber security incidents, based on the incident type, impact, and associated level of risk.

(5) Document in their PCSPs processes for handling information disseminated by CIAC, including procedures for responding proactively to alerts, consequence analyses, and corrective actions. Implementing procedures will be documented in their subordinate organizations' CSPPs and/or system security plans.

c. Restore and Improve.

(1) Ensure that IPWAR procedures are integrated into and tested periodically with the Primary DOE Organization's contingency plan. The contingency plan should include a description of or reference to the IPWAR procedures that would be followed to ensure that the system will continue to have incident protection if a disaster occurs.

(2) Measure the implementation of DOE IPWAR policy requirements within the Primary DOE Organization through performance measures.

(3) Disseminate DOE and external IPWAR-related methods to subordinate organizations.

(4) Identify IPWAR-related methods within the Primary DOE Organization to be shared with DOE via the Office of Cyber Security.

PRIMARY DOE ORGANIZATIONS TO WHICH DOE M 205.1-1 IS APPLICABLE

Office of the Secretary
Office of the Chief Information Officer
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Office of Counterintelligence
Departmental Representative to the Defense Nuclear Facilities Safety Board
Office of Economic Impact and Diversity
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 Hearings and Appeals
Office of Independent Oversight and Performance Assurance
Office of the Inspector General
Office of Intelligence
Office of Legacy Management
Office of Management, Budget and Evaluation and Chief Financial Officer
National Nuclear Security Administration
Office of Nuclear Energy, Science and Technology
Office of Policy and International Affairs
Office of Public Affairs
Office of Security
Office of Security and Performance Assurance
Office of Science
Secretary of Energy Advisory Board
Office of Energy Assurance
Office of Electric Transmission and Distribution
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

CONTRACTOR REQUIREMENTS DOCUMENT
DOE M 205.1-1, *INCIDENT PREVENTION, WARNING, AND RESPONSE (IPWAR) MANUAL*

Regardless of the performer of the work, the contractor is responsible for complying with the requirements of this Contractor Requirements Document (CRD) and for flowing down those requirements to subcontractors at any tier to the extent necessary to ensure contractor compliance with the requirements. In doing so, the contractor must not flow down requirements unnecessarily or imprudently. That is, the contractor will ensure that it and its subcontractors comply with the requirements of this CRD and incur only those costs that would be incurred by a prudent person in the conduct of competitive business.

This CRD supplements requirements in the CRD for DOE O 205.1, *Department of Energy Cyber Security Management Program,* dated 3-21-03, including requirements for cyber resource protection, risk management, program evaluation, and cyber security plan development and maintenance.

The contractor must ensure that all information systems used by its employees or facilities under its control satisfy or comply with the requirements listed below.

1. CATEGORIZING CYBER SECURITY INCIDENTS AND ATTEMPTED INCIDENTS. Cyber security incidents must be characterized and categorized according to their potential to cause damage to information and information systems based on two criteria: incident type and system impact category.[1] The criteria are used in combination to determine the time frame for reporting incidents to the Computer Incident Advisory Capability (CIAC). This CRD establishes two incident types (Type 1 and Type 2) and three categories of system impact (low, moderate, and high), which are described below.

   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 the Type 1 incidents currently defined (see also DOE M 205.1-1, Attachment 4, Definitions).

         (a) *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.

         (b) *Web Site Defacement*. All instances of a defaced Web site must be reported.

[1]The security categorization of systems established by this CRD is based on National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

(c) *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.

(d) *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 by the heads of Primary DOE Organizations.

(e) *Critical Infrastructure Protection (CIP)*. Any activity that adversely affects an asset identified as critical infrastructure must be reported. CIP assets are determined by the heads of Primary DOE Organizations.

(f) *Unauthorized Use*. Unauthorized use should be construed as any activity that adversely affects an information system's normal, baseline performance and/or is not recognized as being related to DOE's mission. For example, unauthorized use can be using a DOE computer to obtain DOE data without authorization. Unauthorized use can involve using DOE's systems to break the law. 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's computers; or using illegal (or misusing copyrighted) software images, applications, data, and music.

(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. The following are the Type 2 incidents currently defined.

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

(b) *Reconnaissance Activity.* Persistent surveillance probes and scans are those that stand out above the daily noise level and represent activity that is designed to collect information about vulnerabilities in a network. The Primary DOE Organization determines the standard for collecting data on surveillance probes and scans of subordinate sites and communicate this information to the contractor point of contact.

b. System Impact Categories. System impact 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. System impact 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. Performing this impact analysis is a fundamental step in risk assessment.

(1) Low Impact. Loss of system confidentiality, integrity, and availability could be expected to have a limited adverse effect on DOE operations, assets, or individuals, requiring minor corrective actions or repairs.

(2) Moderate Impact. Loss of system confidentiality, integrity, and availability could be expected to have a serious adverse effect on DOE operations, assets, or individuals, including significant degradation or major damage, requiring extensive corrective actions or repairs.

(3) High Impact. Loss of system confidentiality, integrity, and availability could be expected to have a severe or catastrophic adverse effect on DOE operations, assets, or individuals. The incident could cause the loss of mission capability for a period that poses a threat to human life or results in the loss of major assets.

2. REPORTING CYBER SECURITY INCIDENTS. Departmental incident reporting procedures can be found at the CIAC Web site (www.ciac.org). Requirements for incident reporting must be documented in the Primary DOE Organization's Program Cyber Security Plan (PCSP). Organizations reporting cyber security incidents for national security systems must also follow the requirements outlined in DOE O 471.4, *Incidents of Security Concern*, dated 3-17-04.

a. Incident Discovery. When a cyber security incident has occurred or is suspected to have occurred, the affected site will immediately examine and document the pertinent facts and circumstances surrounding the incident. (Note: the initial investigation should be completed within 24 hours.)

b. Incident Reporting and Investigating. Once it is determined an incident has occurred, the incident must be categorized according to incident type and category of system affected and reported to CIAC within the time frames indicated in Table 1, in accordance with the process established by the Primary DOE Organization.

c. No Incident. If it is determined that an incident did not occur, no reporting actions are necessary. However, all evaluated and suspected incidents must be documented and local files retained.

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

	System Impact Category		
Incident Type	**Low**	**Moderate**	**High**
Type 1	Within 4 hours[2]	Within 1 hour	Within 1 hour
Type 2	Within 1 week	Within 24 hours	Within 24 hours

d. Monthly Reports. The site must issue a monthly report if it has experienced any reportable successful or attempted cyber security incidents during the previous month. It must also report if it has had no incidents (negative reporting). The reporting process is be documented in the Primary DOE Organization's PCSP.

e. Reporting to the Office of Inspector General. Contractors must inform the Office of the Inspector General of all Type 1 incidents consistent with the time frames indicated in Table 1. Reporting incident information to the Office of Inspector General must be done according to the line of reporting procedures established in the PCSP of the Primary DOE Organization.

f. Reporting to the Office of Security. All DOE organizations must inform the Office of Security for incidents involving national security systems in accordance with the requirements outlined in DOE O 471.4, *Incidents of Security Concern*, dated 3-17-04.

g. Reporting to the Office of Counterintelligence. All DOE organizations must inform the Office of Counterintelligence whenever there is suspicion of involvement of a foreign government, entity, or national. Organizations should take appropriate precautions when reporting these incidents and must follow the procedures outlined in DOE O 471.4, *Incidents of Security Concern,* dated 3-17-04, for reporting all incidents involving national security systems.

h. Automated Systems. Automated systems may be used for reporting if reporting by such systems complies with the requirements of this CRD.

3. CYBER ALERTS.

a. CIAC is the official DOE point of contact for prompt dissemination of information provided in alerts received from external organizations. In addition, CIAC provides DOE responses to national centers, as required. The timing of distribution will be commensurate with the significance of the information.

[2]Reporting timeframes begin at the point of incident identification.

b. If CIAC issues an alert, CIAC will notify sites of the alert by contacting the site incident response on-call pager number. Upon notification of the alert, the contractor security points of contact will—

(1) acknowledge the receipt of the alert within 4 normal business hours and

(2) execute the required analyses and appropriate corrective actions and report the actions taken, or provide justification for why actions were not taken, in accordance with the Primary DOE Organization's PCSP.

4. UPDATING CYBER SECURITY PATCHES. Security patches must be installed regularly and in a timely manner to help prevent intrusions. The Primary DOE Organization's designated approving authority (DAA) must approve decisions not to apply security patches to systems, as in the case where stability may be sacrificed (and thus availability). All patches and updates must be reviewed for site applicability and 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 United States Computer Emergency Readiness Team Web site (http://www.us-cert.gov), and trusted vendors.

5. CYBER SECURITY INCIDENT PREPAREDNESS/RESPONSE AND CONTINGENCY PLANS. Because of the interrelationship of cyber security incident preparedness/response and continuity of operations, IPWAR procedures should be integrated into, and tested periodically with, the Primary DOE Organizations' information system contingency plans. Contingency plans should include a description of or reference to the IPWAR procedures that would be followed to ensure that the system will continue to have incident protection if a disaster occurs. Contractors are responsible for supporting this requirement as it is outlined in the Primary DOE Organization's PCSP and subordinate security plans.

6. CYBER SECURITY INCIDENT TRAINING. Contractors are responsible for complying with the training requirements established in the Primary DOE Organization's PCSP.

CONTRACTOR REQUIREMENTS DOCUMENT (CRD) APPLICABILITY

The CRD for DOE M 205.1-1 is intended to apply to the site/facility management contracts applicable to the following sites/facilities.

Lawrence Berkeley National Laboratory

Pacific Northwest National Laboratory

Brookhaven National Laboratory

Sandia National Laboratories

National Renewable Energy Laboratory

Stanford Linear Accelerator Center

Bettis Atomic Power Laboratory

Argonne National Laboratory

Idaho National Engineering & Environmental Laboratory

Thomas Jefferson National Accelerator Facility

Ames National Laboratory

Oak Ridge National Laboratory

Knolls Atomic Power Laboratory

Lawrence Livermore National Laboratory

Los Alamos National Laboratory

Savannah River Site

Princeton Plasma Physics Laboratory

Fermi National Accelerator Center

West Valley Project

Strategic Petroleum Reserve

Oak Ridge Y-12 National Security Complex

Pantex Plant

Waste Isolation Pilot Plant

Nevada Test Site

Kansas City Plant

National Civilian Radioactive Waste Program (Yucca Mountain)

Hanford Environmental Restoration

Oak Ridge Environmental Management

Mound Environmental Management Project

Project Hanford

River Protection Project Tank Farm Management

Rocky Flats

Fernald Environmental Management Project

Grand Junction Technical & Remediation Services

Grand Junction Facilities & Operations Services

Oak Ridge Institute of Science & Education

Occupational Health Services at the Hanford Site

DEFINITIONS

The following terms are specific to the DOE Classified and Unclassified Cyber Security Program. Some definitions are followed by a citation indicating the source. (Citations are given in full on first use and are abbreviated thereafter.) Where no citation appears, the definition has been derived from several sources or from common usage. Many definitions are from the National Security Telecommunications and IT Investments Security Committee's National Information Technology Investments Security (INFOSEC) Glossary. Other definitions may be found in the DOE *Safeguards and Security Glossary of Terms*, which is available online at http://www.directives.doe.gov/pdfs/nnglossary.

Accreditation—Formal declaration by a designated accrediting authority (DAA) that an information system is approved to operate in a particular security mode at an acceptable level of risk based on the implementation of an approved set of technical, managerial, and procedural safeguards.

Audit—Independent review and examination of records and activities to assess the adequacy of system controls; to ensure compliance with established policies and operational procedures; and to recommend necessary changes in controls, policies, or procedures.

Alert—Time-critical message or posting to notify DOE organizations that they are in imminent danger of attack. Alerts require acknowledgment of receipt by the DOE organization's primary or alternate point of contact within 4 business hours of successful delivery. The designation "alert" is used for notifications about attacks at other DOE sites, Federal agencies, or organizations. When a Computer Incident Advisory Capability (CIAC) alert is issued, DOE organizations and contractors are requested to review activities at their respective sites for the actions or events described in the alert and provide appropriate notifications if similar activities are found.

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

Certification—Comprehensive evaluation of the technical and nontechnical security safeguards of an information system to support the accreditation process that establishes the extent to which a particular design and implementation meet a set of specified security requirements.

Classified Information—Information that is classified as Restricted Data or Formerly Restricted Data under the Atomic Energy Act of 1954, as amended, or information determined to require protection against unauthorized disclosure under Executive Order 12958 or prior Executive orders and is marked to indicate its classified status when in documentary form.

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—Protection of information technology investments against unauthorized access to or modification of information, whether in storage, processing, or transit; against loss of accountability for information and user actions; and against the denial of service to authorized users, including those measures necessary to protect against, detect, and counter such threats.

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. Adverse events include, but are not limited to, attempts (successful or persistent) to gain unauthorized access to an information system or its data; unwanted disruption or denial of service; unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent. Examples include insertion of malicious code (for example, viruses, Trojan horses, or back doors), unauthorized scans or probes, successful or persistent attempts at intrusion, and insider attacks.

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

Primary DOE Organizations—Refer to those listed in DOE M 205.1-1, Attachment 1.

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.

National Security System— any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, the function, operation, or use of which involves intelligence activities;

involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions; or is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. National security systems do not include systems that are to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). (FISMA, Sec. 3542). National Security Systems include all systems classified under the Atomic Energy Act of 1954 and Executive Order 12958.

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).

Risk Management—Process of identifying and applying countermeasures commensurate with the value of the assets protected based on a risk assessment.

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.

Threat—Any circumstance or event with the potential to adversely impact an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. The following are examples.

- External security threats, which come from individuals who use technical knowledge or social engineering to gain unauthorized access (either via remote or gained local access) to perform malicious activity in cyber systems.

- Insider security threats (whether intentional or unintentional) with potential to be more serious than an external threat because the perpetrator of malicious activity has authorized access to the system.

- Foreign access threat (either remote or internal) to the information environment requiring assessment to ensure that access by foreign nationals to DOE cyber systems is approved by an official designated by the DOE site manager or line-level organization accountable for the approval decision.

- Portable electronic devices, including laptop computers; palm devices; and cell phones capable of receiving, storing, or transmitting data in an electronic format. Issues of concern include data aggregation, theft, and radio frequency/infrared interconnectivity.

- Mosaic threat that classified information or information requiring enhanced protection will be derived by combining open source information made separately available, perhaps by different organizations.

Unclassified—Designation for information, document, or material that has been determined not to be classified or that has been declassified by proper authority.

Unclassified Controlled Information—Unclassified information that may be exempt from public release under the Freedom of Information Act or other statute (e.g., Official Use Only information, Unclassified Controlled Nuclear Information).

Vulnerability—Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited as follows.

- Major vulnerability—if discovered and exploited, could reasonably be expected to result in a successful attack causing serious damage to the national security.

- Unspecified major vulnerability—weakness in a system or organization's defenses that could be exploited and is specified in no greater detail than the specific security system (or one of its major components) when it occurs.

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.

ACRONYMS

CIO	Chief Information Officer
CIAC	Computer Incident Advisory Capability
CIP	critical infrastructure protection
CIRT	Computer Incident Response Team
CRD	Contractor Requirements Document
CSPP	Cyber Security Program Plan
FISMA	Federal Information Security Management Act
IPWAR	incident prevention, warning, and response
IT	information technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PCSP	Program Cyber Security Plan
SP	Special Publication
US-CERT	United States Computer Emergency Readiness Team

SAMPLE CYBER INCIDENT RESPONSE PLAN

This sample plan consists of three sections. The first section details the plan's scope, the second describes establishment of roles and responsibilities regarding the Computer Incident Response Team (CIRT), and the final section presents a formal set of procedures for reporting and handling information technology (IT) security incidents. The cyber incident response plan should be included or referenced in the Primary DOE Organization's Program Cyber Security Plan document.

1. PLAN SCOPE. Before starting to develop the plan, the Primary DOE Organization should determine what the plan will cover and the personnel responsibilities as this will affect the procedures and processes used to handle a computer security incident. The Primary DOE Organization should also consider any external connections, including how an incident might affect another Agency, contractor, or Primary DOE Organization that is connected in some way to the affected system or network. The Primary DOE Organization also should state within the plan how the organization works with its IT and security staffs and the types of systems the plan will cover. This will help determine which job positions the incident response team will need to include.

2. COMPUTER INCIDENT RESPONSE TEAM. The organization's written procedures must identify who will perform the procedures. Accordingly, the response plan should describe the makeup and roles and responsibilities of the CIRT. Depending on the size and structure of the Primary DOE Organization, multiple tiers of CIRTs may be required to effectively address incidents, both across the organization and within subordinate organizations. In such cases, the membership of each team should be consistent with competencies appropriate to the team's tier. The team should be composed of a core group, which will be involved in all incidents, and a group of platform and system specialists, who will participate as incidents require.

   a. The Core Group. The core group members may include the IT security program manager [or the information system (IS) security manager]; representatives from the Inspector General's office (OIG), public relations (PR), and human resources or personnel; and someone with an investigative or forensics background. The organization can add personnel to the core group as needed.

      (1) *IT Security Program Manager*. This person is the overall head of the organization's IT security program and should be the CIRT leader. In most cases, he or she will appoint someone to be the IS security manager, who will run the day-to-day incident response team operations. This leaves the security program manager free to manage the organization's overall IT security. In the case of a multitier organizational structure, an IS security manager, who will lead the local incident response team, should be appointed for each subordinate organization. As the team leader, the IT security program manager or IS security manager will be the director of each incident investigation. He or she will decide whether additional personnel are required for an investigation, ensure that all

procedures are followed, and decide whether outside assistance is required, as approved by upper management. The IT security program manager also authorizes the release of any information about the incident, again, with upper management consent. However, he or she is not the organization's media spokesperson.

(2) *Inspector General Representative*. An OIG representative may serve as an informal advisor to the CIRT and a supplemental liaison with local, State, Federal, and internal law enforcement. The OIG representative will not provide legal advice or operational direction.

(3) *Public Relations Representative*. PR should be centralized, with information being released only by the Department's PR office. The PR representative is the sole point of contact for the media for release of information, as authorized by the IT security program manager.

(4) *Human Resources or Personnel Representative*. There are various reasons for including a human resources/personnel representative on the team. This person should ensure that the team does not violate employees' rights (for example, privacy) during investigations. In addition, this representative should make sure that appropriate disciplinary methods are used if an employee is found to be the source of an incident.

(5) *Information Technology Investigative/Forensic Expert*. The IT investigative/forensic expert should ensure that the investigation is performed in a methodical manner and that evidence is collected and stored properly. This expertise will assist in the overall handling of the incident and will be especially helpful if the organization wishes to prosecute the individual responsible for the incident. If a prosecution is pursued, the evidence must be collected and handled so that it can be used in the criminal case. This proper handling includes keeping the chain of evidence clean, secure, and verifiable.

b. Incident-Specific Team Members. Other personnel may be added to the CIRT team on an as-needed basis. Although the requirement for additional personnel will depend on the specific incident to be handled, all such personnel must be knowledgeable about the system under attack. Key personnel include the IS security officer, system administrators, communication specialists, system developers, database administrators, and the system owner. Other personnel may also be included.

(1) *Information System Security Officer*. Each general support system or major application should be assigned an IS security officer who ensures that the system is in line with the organization's IT security policy and guidelines. This officer assists the core group in handling an intrusion by stating how the entire system should be set up and configured.

(2) *System Administrators*. System administrators who administer the hardware on which the system runs are critical in incident handling, because of their intimate knowledge of the system hardware, the operating system configuration, and the services that run on the system.

(3) *Network Specialists*. These specialists are essential members of an incident response team because of their knowledge of the network and its configuration, including the firewall configuration if a firewall is used. They will know where a compromised system is connected to the network and whether it has any other connections to the Internet that are not protected by the firewall. They also know how the routers, bridges, and gateways are configured and where they are located within the network. In most cases, these specialists also monitor the intrusion detection system, if the organization uses one.

(4) *System Developers*. System developers know the intricacies of the system or application. Therefore, they know whether the compromised system or application is not running properly and whether it has been modified.

(5) *Database Administrators*. If the compromised system uses a database, database administrators must evaluate whether changes have been made to the database structure or configuration. They can also determine whether any database-specific programs (for example, stored procedures or queries) have been modified.

(6) *System Owner*. It is important that the system owner, if not the instigator of the incident, be part of the incident handling team for several reasons. First, because the owner knows exactly how critical the system is to the organization's mission, he or she can determine how soon an intrusion session should be terminated and whether the system should be taken off the production server. The owner also knows whether a backup system must be put into production immediately or the system can be kept down until the main system is validated and any system vulnerabilities are corrected. Finally, the system owner knows the proper data format and can tell whether the data makes sense and provides the proper output.

c. Response Team Duties. The function of the CIRT is to handle information security incidents as they occur, following the procedures of the IT security program. If an incident occurs, the team members ensure that it is handled as quickly as possible and that it does not affect the security of other systems and applications. In addition, if there is an incident, they should know whom to contact, even if only for informational purposes. The response team also should have procedures for controlling the release of information within the organization.

3. INCIDENT REPORTING PROCEDURES. A standard process for reporting incidents should be developed as part of the formal reporting procedures. This process should

include a standardized form that can assist personnel in reporting a suspected computer-related incident. The form should provide the following information:

a. name of organization;

b. contact information for this incident;

c. physical location of affected computer/network;

d. date incident occurred;

e. time incident occurred;

f. which critical infrastructure was affected;

g. type of incident (for example, intrusion, denial of service, Web site defacement);

h. Internet protocol (IP) address of affected system;

i. IP address of apparent attacker;

j. operating system of affected host;

k. functions of affected host;

l. number of hosts affected;

m. suspected method of intrusion/attack;

n. suspected perpetrators and/or possible motivations;

o. evidence of spoofing;

p. system or 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;

t. what actions have been taken;

u. with whom the information can be shared (for example, 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 intrusion;

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

y. last time the system was modified or up.

The incident reporting procedures should stipulate to whom the reporter should send the completed incident reporting form.

4. INCIDENT HANDLING PROCEDURES. Once an incident has been reported, the procedures should stipulate how it should be investigated and handled. These procedures

should reflect the requirements of Federal legislation, Office of Management and Budget memorandums and circulars, and National Institute of Standards and Technology standards. The procedures should also implement the processes and requirements identified in DOE M 205.1-1, *Incident Prevention, Warning, and Response (IPWAR) Manual,* dated 9-30-04, and other applicable DOE policy.

SAMPLE, "AT A GLANCE," INCIDENT SIGNS AND REPORTING WORKSHEET

DOE promotes the education and awareness of all users to the threat posed by unauthorized disclosure of information. This attachment provides sample information that can be distributed to users during awareness training. The signs list helps to promote ongoing awareness of activities that may, initially, be disregarded as simple system errors but actually point to a potential incident.

Signs of an Incident

You may be able to reduce the impact of an incident across your organization by reporting suspicious or anomalous events as soon as they are detected. While these events don't always involve a security incident, they may. If you see multiple events occurring simultaneously, you may want to alert the help desk or your supervisor. Common system areas and corresponding abnormal events include the following.

a. Unexplained modification or deletion of data

b. Unexplained discovery of new files or unfamiliar filenames

c. Multiple unsuccessful and unexplained logon attempts or your account locked

d. Unauthorized creation of new user accounts

e. Unexplained or suspicious system entries

f. Missing or unusually full system logs

g. Attempts over a period of time targeted against a specific location (historical analysis)

h. Unauthorized modification of file lengths and/or dates

i. Unauthorized or unexplained attempts to write to system files or alter system files

j. Activation of a system alarm or similar indication of an intrusion

k. Denial of service attack on the system

l. Multiple users logged on to a single account

m. Entire system crashes

n. Unauthorized operation of a program, known as a "sniffer device," to monitor network traffic

o. Usage of attack scanners or remote requests for information about systems and/or users

p. Unusual network activity after normal operating hours

q. Abnormal number of locked accounts

r. Unauthorized scans of ports or unusually heavy traffic to a specific port

The "do" and "don't" lists provided below are examples of those that a Primary DOE Organization might use in developing its user incident action and reporting checklist. These lists

are provided as examples and starting points for Primary DOE Organizations to use in developing and sharing ideas for comprehensive user checklists.

DO

- Remain calm. Take your time and follow all steps to handle the incident properly.
- Keep detailed notes. Take step-by-step notes and write down observations with times of occurrence as the incident response progresses.
- Leave the system as is! For investigative forensic purposes, it is imperative that the system remains in the same condition as when the incident was discovered. Leave the system in operation until appropriately trained law enforcement personnel can respond.
- Report immediately. Contact your local information security office for guidance. You may also contact DOE Computer Incident Advisory Capability (CIAC) at—

DOE-CIAC Web site	http://www.ciac.org/ciac
DOE-CIAC E-mail	ciac@ciac.org
DOE-CIAC Hotline	925-422-8193
STU-III Phone	925-423-2604

  In an emergency, you may also contact the United States Computer Emergency Readiness Team (US-CERT): http://www.us-cert.gov.

- Notify the appropriate individuals. Management should be informed so proper decisions can be made.
- Prepare to find more than you are looking for. You never know what you may find when looking at an employee's computer that could lead to evidence of other computer crimes.

DON'T

- Rush! Trying to respond too quickly may cause unnecessary mistakes to be made.
- Power down the machine. Valuable information regarding the incident could be lost.
- Use a video camera. It may disclose DOE-sensitive information if the case is taken to court.
- Wait to respond. Waiting to respond can cause evidence to be lost, and staff may forget details needed to answer important questions.
- Run/install programs on the system. This could overwrite potential evidence on the system.
- Underestimate the incident scope. If you underestimate the scope of the incident, you may miss crucial evidence.
- Keep information from the decision makers. If management lacks the necessary information to make informed decisions, the response may not be handled in the most effective manner.