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

NOTICE

DOE N 205.4

Approved: 3-18-02
Expires: 3-18-03

SUBJECT: HANDLING CYBER SECURITY ALERTS AND ADVISORIES AND REPORTING CYBER SECURITY INCIDENTS

1. OBJECTIVES.

   a. To establish Department of Energy (DOE) requirements and responsibilities for reporting cyber security incidents involving classified and unclassified systems and responding to cyber security alerts and advisories.

   b. To implement requirements of DOE N 205.1, *Unclassified Cyber Security Program*, and DOE M 471.2-2, *Classified Information Systems Security Manual*.

2. CANCELLATION. This Notice cancels Chapter III, Section 8, Incident Reporting, of DOE M 471.2-2.

3. APPLICABILITY.

   a. DOE Elements. This Notice applies to all DOE elements (collectively referred to as line management), including the National Nuclear Security Administration (NNSA), that have access to DOE cyber systems.

   b. Contractors. The Contractor Requirements Document (CRD), Attachment 1, sets forth requirements that apply to DOE/NNSA contractors and subcontractors that have access to DOE cyber systems. Contractor compliance will be required to the extent set forth in a contract.

   NOTE: This Notice does not address contamination of unclassified systems with classified information (see DOE N 471.3, *Reporting Incidents of Security Concern*, and DOE M 471.2-2).

4. REQUIREMENTS.

   a. Implementation. Line management must implement the responsibilities and requirements contained in this Notice within 90 days of its issuance. Contractors who provide direct support to line management will report through the line management. Program organizations must not issue direction or guidance on cyber security matters directly to the sites that are managed by a lead program secretarial office (LPSO); such matters must be coordinated with the site's LPSO.

DISTRIBUTION:
All Departmental Elements

INITIATED BY:
Office of the Chief Information Officer

The Office of the Chief Information Officer (OCIO) will be the point of contact for the Headquarters site.

b. Reportable Cyber Security Incidents. All DOE organizations will develop and document procedures for reporting cyber security incidents in their Cyber Security Program Plans (CSPPs) or similar documents for classified systems. DOE organizations will report cyber security related incidents that are significant or unusually persistent and meet one or more of the following criteria:

(1) Unauthorized Access. All attempts at unauthorized access, whether or not they are successful, even if unauthorized access is suspected but not yet proven.

(2) Malicious Code. Instances of malicious code such as viruses, Trojan horses, or worms.

(3) Denial of Service. Denial of service (successful or unsuccessful) that affects or threatens to affect a critical service or denies access to all or large portions of a site's network.

(4) Scans and Probes. Unauthorized network scans, probes, and attempted denial of service.

c. Cyber Security Incident Reporting Protocol.

(1) All sites will inform Computer Incident Advisory Capability (CIAC) of all reportable cyber security incidents upon discovery. The incident-reporting procedure is available at http://cio.doe.gov/cyberhome.htm.

(2) Line management or sites [depending on the process identified by Line Management in paragraph 5c(4)] will inform the Office of Inspector General of attacks or activities, including unsuccessful attempts at unauthorized access, malicious code, and denial-of-service events, if there is reason to suspect that the attempts are significant or unusually persistent.

d. Cyber Alerts, Advisories, and Bulletins.

(1) CIAC is the official DOE point of contact for prompt dissemination of information provided in alerts, advisories, notices, bulletins, or other cyber security information from external organizations and any CIAC-developed information. The timing of distribution will be commensurate with the significance of the information.

(2) Line management will ensure that the field implements a consistent and effective process for handling information disseminated by CIAC, including processes for consequence analysis and corrective actions. CIAC notification is not required to act on information from vendors and recognized non-Government resources such as the Computer Emergency Response Team (CERT). These processes will be documented in the CSPP or similar document for classified systems.

5. RESPONSIBILITIES.

a. Office of the CIO.

(1) Manages Department-wide cyber security incident reporting and response activities, in coordination with the Office of Counterintelligence or the Office of Inspector General, as circumstances warrant.

(2) Provides guidance to appropriate DOE officials, who direct CIAC.

(3) Disseminates information on cyber security, as appropriate, to line management without attribution to a site unless the announcement has been coordinated in advance with line management, including site senior management.

(4) Provides information and/or reports to line management, as requested.

(5) Maintains emergency contact information for Federal and contractor cyber security points of contact.

(6) Accepts responsibility for reporting at the Headquarters site.

b. Computer Incident Advisory Capability (CIAC).

(1) When directed by appropriate DOE officials, provides cyber security incident response, watch, and warning capabilities; analysis; and assistance reviews for the Department.

(2) Serves as the Departmental cyber incident reporting point of contact for the receipt of alerts, advisories, notices, bulletins, or other cyber security information from both DOE and external organizations. Logs all cyber security incident reports, acknowledges receipt, and assigns incident numbers for those incidents. Works with the Office of the Associate CIO for Cyber Security to determine if conditions indicate that a multiple-site event that warrants reporting to the Offices of Inspector General or Counterintelligence has occurred or is emerging.

(3) Provides summary cyber security incident information to external organizations, such as the Federal Computer Incident Response Capability (FedCIRC) and the National Infrastructure Protection Center (NIPC), in accordance with Federal law. The reporting will not be attributed to any site unless the Office of the Associate CIO for Cyber Security coordinates the announcement with line management, including site senior management, in advance

(4) Provides line management with immediate and effective technical and nontechnical assistance (tools, methods, and guidance) in response to a cyber security incident when requested. When requested, provides analysis and supports the notifying organizations.

(5) Posts unclassified alerts and advisories on the DOE limited access server.

(6) Notifies line management and field facility organizations in a timely manner, through primary and alternate points of contact, that an alert or advisory has been posted for their review and action.

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

c. Line Management.

(1) Establishes controls to ensure that the requirements of this Notice are implemented and documented in the CSPPs or similar documents for classified systems in the field. All DOE organizations will work with CIAC to determine the severity or significance of a cyber security incident.

(2) Ensures that a process is established for the field to report significant or unusually persistent cyber security incidents to CIAC. When appropriate, works with CIAC to analyze the effect of cyber security incidents, determine who should be informed, and decide how to escalate the issue within the line organization's management. The process must ensure that any comprise of classified information is reported in accordance with DOE N 471.3.

(3) Ensures compliance with DOE 5670.3, *Counterintelligence Program*, for counterintelligence related events.

(4) Establishes a process for reporting incidents (based on the criteria in paragraph 4b) to the Technology Crimes Section of the Office of Inspector General in accordance with DOE O 221.1 and DOE N 221.7, *Reporting Fraud, Waste, and Abuse*.

(5) Ensures that appropriate action is taken regarding cyber security alerts and advisories.

(6) Ensures that significant or unusually persistent cyber security incidents are reported to program management, site management, the legal authority, and/or the investigating organization(s), as appropriate.

(7) Provides emergency contact information to Office of the Associate CIO for Cyber Security for Federal and contractor reporting in accordance with established site policy.

6. REFERENCES.

a. DOE N 205.1, *Unclassified Cyber Security Program*, dated 7-26-99.

b. DOE N 221.7, *Reporting Fraud, Waste, and Abuse*, dated 7-12-01.

c. DOE N 471.3, *Reporting Incidents of Security Concern*, dated 4-13-01.

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

e. DOE M 471.2-2, *Classified Information Systems Security Manual*, dated 8-3-99.

f. DOE 5670.3, *Counterintelligence Program*, dated 9-4-92.

g. Government Information Security Reform Act, Title X, subtitle G of the 2001 Defense Authorization Act (Public Law 106-398).

h. Computer Fraud and Abuse Act 1986 (US), Title 18 U.S.C., Crimes and Criminal Procedure, section 1030, Fraud and Related Activity in Connection with Computers.

i. OMB Circular A-130, Management of Federal Information Resources; Appendix III, Security of Federal Automated Information Resources.

j. Computer Security Act of 1987.

7. DEFINITIONS.

a. Alert. A time-critical message or posting to notify organizations that they are in imminent danger of attack. Alerts require acknowledgment of receipt from the DOE organization primary or alternate point of contact within 4 hours of successful delivery. This designation will be used for notifications about attacks

at other DOE sites, Federal agencies, or organizations. In addition, when a 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.

b. Advisory. A critical message or posting requiring acknowledgment from the DOE organization primary or alternate point of contact within 24 hours of delivery. This designation is used when the potential exists for a root compromise by a serious vulnerability that is actively being exploited and affects hardware or software widely used by DOE or when the potential for widespread consequences exists. These are usually sent by e-mail or facsimile (fax); sometimes urgency will also require site contact by phone or pager to ensure awareness of the advisory and immediate action.

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

d. Cyber Security Incident. Any adverse event that threatens the security of information resources. Adverse events may include compromises of integrity, denial-of-service attacks, compromises of confidentiality, loss of accountability, or damage to any part of the system. Examples include the insertion of malicious code (e.g., viruses, Trojan horses, or back doors), unauthorized scans or probes, successful and unsuccessful intrusions, and insider attacks.

BY ORDER OF THE SECRETARY OF ENERGY:

FRANCIS S. BLAKE
Deputy Secretary

CONTRACTOR REQUIREMENTS DOCUMENT

DOE N 205.4, *Handling Cyber Security Alerts and Advisories and Reporting Cyber Security Incidents*

Regardless of the performer of the work, Department of Energy (DOE), including the National Nuclear Security Administration (NNSA), contractors are responsible for compliance with the requirements of this Contractor Requirements Document (CRD). The contractor is responsible for flowing down the requirements of this CRD to subcontracts at any tier to the extent necessary to ensure the contractor's compliance with the requirements. When responding to cyber security alerts and advisories and reporting cyber security incidents—

1. Reportable Cyber Security Incidents. Contractors must develop and document procedures for reporting cyber security incidents in their Cyber Security Program Plans (CSPPs) or similar documents for classified systems. Contractors must report cyber security related incidents that are significant or unusually persistent and meet one or more of the following criteria:

   a. Unauthorized Access. All attempts at unauthorized access, whether or not they are successful, even if unauthorized access is suspected but not yet proven.

   b. Malicious Code. Instances of malicious code such as viruses, Trojan horses, or worms.

   c. Denial of Service. Denial of service (successful or unsuccessful) that affects or threatens to affect a critical service or denies access to all or large portions of a site's network.

   d. Scans and Probes. Unauthorized network scans, probes, and attempted denial of service.

2. Cyber Security Incident Reporting Protocol. Contractors will inform their Federal line management (DOE elements, including NNSA, that have access to DOE cyber systems) and the Computer Incident Advisory Capability (CIAC) of all reportable cyber security incidents upon discovery. Contractors, at the direction of line management, will work with CIAC to determine the severity or significance of a cyber security incident. The incident reporting procedure is available at http://cio.doe.gov/cyberhome.htm.

   Federal line management or contractors (depending on the process identified by line management) will inform the Office of Inspector General of attacks or activities, including unsuccessful attempts at unauthorized access, malicious code, and denial-of-service events, if there is reason to suspect that the attempts are significant or unusually persistent.

3. Cyber Alerts, Advisories, and Bulletins. CIAC is the official DOE point of contact for prompt dissemination of information provided in alerts, advisories, notices, bulletins, or other cyber security information from external organizations and any CIAC-developed information. The contractor will implement a consistent and effective process for handling information disseminated by CIAC, including processes for consequence analysis and corrective actions. CIAC notification is not required to act on information from vendors and recognized non-Government resources such as the Computer Emergency Response Team (CERT). These processes will be documented in the contractor's CSPP or similar document for classified systems.

4. DEFINITIONS.

a. Alert. A time-critical message or posting to notify organizations that they are in imminent danger of attack. Alerts require acknowledgment of receipt from the DOE organization primary or alternate point of contact within 4 hours of successful delivery. This designation will be used for notifications about attacks at other DOE sites, Federal agencies, or organizations. In addition, when a 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.

b. Advisory. A critical message or posting requiring acknowledgment from the DOE organization primary or alternate point of contact within 24 hours of delivery. This designation is used when the potential exists for a root compromise by a serious vulnerability that is actively being exploited and affects hardware or software widely used by DOE or when the potential for widespread consequences exists. These are usually sent by e-mail or facsimile (fax); sometimes urgency will also require site contact by phone or pager to ensure awareness of the advisory and immediate action.

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

d. Cyber Security Incident. Any adverse event that threatens the security of information resources. Adverse events may include compromises of integrity, denial-of-service attacks, compromises of confidentiality, loss of accountability, or damage to any part of the system. Examples include the insertion of malicious code (e.g., viruses, Trojan horses, or back doors), unauthorized scans or probes, successful and unsuccessful intrusions, and insider attacks.