




The Deputy Secretary of Energy
Washington, DC 20585

February 18, 2004

MEMORANDUM FOR HEADS OF DEPARTMENTAL ELEMENTS

BRUCE M. CARNES, ASSOCIATE DEPUTY
SECRETARY

FROM: KYLE E. McSLARROW 

SUBJECT: Cyber Security Incident Reporting

This memorandum serves as interim policy to promote increased cyber security across the Department of Energy and ensure that statutory responsibilities in the area of cyber incident reporting are fulfilled. This policy is effective immediately and applies to all departmental elements and all information systems used or operated by the Department, a contractor, or any other organization on behalf of the Department. Once issued, the new *Incident Prevention, Warning and Response Manual*, which is now in review, will supersede this interim policy.

The importance of incident reporting cannot be overstated. I view it as unacceptable that numerous Inspector General and Office of Independent Assessment and Performance Assurance reports identify the Department's cyber incident reporting program as especially weak. In particular, despite long-standing requirements, less than half of Department of Energy (DOE) field activities report cyber security incidents.

Policy

As detailed in the attachment to this memorandum, each Departmental Element must:

- 1) Continue to report successful and unsuccessful cyber security incidents as required by DOE N 205.4, *Handling Cyber Security Alerts and Advisories and Reporting Cyber Security Incidents*, or
- 2) Monthly, beginning in January 2004, certify in writing to the Office of the Chief Information Officer (OCIO) that all reportable incidents that occurred during the previous calendar month have been reported.

When applicable, certain cyber security incidents must also be reported to the Office of Security, Office of Inspector General, and Office of Counterintelligence, consistent with policies from those organizations.



In carrying out these responsibilities, the DOE Chief Information Officer and the Administrator, National Nuclear Security Administration will coordinate NNSA anticipated actions as prescribed in DOE Order 205.1, *Department of Energy Cyber Security Management Program*.

I will look to the Chief Information Officer to provide me and the Associate Deputy Secretary with regular reports on compliance with this policy.

The degree of compliance with this policy will be monitored as part of the revised DOE quarterly cyber security scorecard. Please direct any questions to Glenn Schlarman, Associate CIO for Cyber Security, or Carol Bales, Deputy Associate CIO for Cyber Security, at 202-586-1090 or by e-mail. To promote efficient and consistent program management, field sites should first consult with their respective Program Office before contacting the OCIO.

Attachment

Interim Procedures for Cyber Incident Reporting

As specified in DOE Order 205.1, *Department of Energy Cyber Security Management Program* and DOE Notice 205.4, *Handling Cyber Security Alerts and Advisories and Reporting Cyber Security Incidents*, procedures for cyber security incident reporting must be documented in each Program Cyber Security Plan and Cyber Security Program Plan.

When faced with attempted or successful cyber security incidents, each system owner must first protect their own system and data to prevent or reduce local damage. As soon as practicable thereafter, to prevent the spread of damage to other systems and organizations, system owners must report to Computer Incident Advisory Capability Office (CIAC) information concerning incidents and common threats and vulnerabilities (e.g., attempted denial of service attacks or the introduction of viruses and worms). Additionally, reporting successful incidents (e.g., root compromises) can help management officials assess the level of security performance and focus on improvement.

All DOE elements must report to CIAC successful and attempted incidents as follows¹:

- 1) One hour after discovery – brief heads up warning of persistent attempted attacks, viruses, worms, etc., (whether or not successful);
- 2) Twenty-four hours after initial heads up – incident details involving moderate and high-risk systems. Moderate and high-risk systems include any system interconnected with other systems and organizations; and
- 3) One week after initial heads up – incident details involving low-risk systems. Among other characteristics, low-risk systems do not interconnect with other systems or organizations.

As necessary, the OCIO (via CIAC) will work with the appropriate program offices to follow-up on specific incidents and compile additional pertinent information. For example, for successful root compromises the OCIO will collect causal data such as whether the compromise resulted from an unpatched system.

Monthly Negative Reports

By the third week of each calendar month, a responsible site official will certify in writing to CIAC that no reportable incidents occurred during the previous calendar month. Certification may be sent via e-mail or fax. Following procedures set forth by the appropriate program offices, copies should also be sent to the site's respective program office.

¹ See CIAC's website for protocols http://www.ciac.org/ciac/CIAC_incident_reporting_procs.html.