



---

## Energy's unclassified networks still open to cyberattack

09/19/08

The Energy Department has failed to implement cybersecurity measures, leaving its unclassified computer systems and data open to hackers and employees who may not have authorization to access certain files, according to an audit report released by the agency's inspector general.

Energy improved some security weaknesses the IG identified in its fiscal 2007 audit, including strengthening configurations of networks and systems, updating security policies and procedures related to laptops, and improving reporting of security incidents. The agency also began including cybersecurity requirements in relevant contracts.

[Comment on this article in The Forum.](#)

But weaknesses still exist, according to the IG, who conducted an evaluation of unclassified systems between February and September. The Office of Independent Oversight performed a separate evaluation of systems that contain sensitive data.

"Security challenges and threats to the Department of Energy's information systems are continually evolving," Inspector General Gregory Friedman wrote in a memorandum. "Adversaries routinely attempt to compromise its information technology assets. As these attacks become increasingly sophisticated, it is critical that the department's cybersecurity protective measures keep pace with the growing threat."

At the time of the IG's evaluation, department sites reported 480 cybersecurity incidents that affected 703 computers to its Computer Incident Advisory Capability, which monitors network security. That was an increase of about 45 percent from the prior year.

In addition, 127 of the incidents involved personal identifiable information, an increase of about 165 percent from those reported in fiscal 2007. Part of the increase may be attributed to increased awareness of security and better reporting, Friedman noted, the Energy Department still must improve security.

The IG [report](#) noted a number of weaknesses in the department's certification and accreditation processes, which is required under the [2002 Federal Information Security Management Act](#). System security plans at five agency sites did not have essential components of the process, such as descriptions of mandatory security controls that help ensure officials have considered and addressed all risks to systems.

Also, the Energy Department had not performed annual self-assessments of mandatory security controls at four sites, and independent assessments of security controls performed at four sites were inadequate. One site failed to properly test security controls, and two sites had not completed certification and assessment for certain systems, despite being identified in previous reports since fiscal 2006.

The IG also reported that the Energy Department failed to inventory all information systems that access the agency's network. FISMA requires agencies to identify all systems the agency uses, including those not operated by the agency, as well as the interfaces between systems. The department began to deploy several reporting tools to identify systems in fiscal 2007, but the agency had not completed the inventory at the time of the audit.

An Energy official said, however, the identification tools were not adequate, because they did not provide a fully automated asset management system that identifies system connections and includes configuration and patch management capabilities.

The department also must tighten access controls, the IG reported. At one agency site, a financial system administrator was granted privileges that were not needed to perform his duties. The privileges allowed the administrator to conduct unauthorized modification to the system or information. Another site allowed unsupervised visitors to connect to the agency's intranet using their own laptops. Such access provides opportunity to probe the network for vulnerabilities, implant malicious code, or remove data without authorization, the report noted.

Similarly, failure to securely configure all systems introduced the potential for exploits. The IG found two Energy sites that used software that was either outdated or not appropriately patched, and a number of department locations neglected to disable unnecessary computer services for publicly accessible Web sites.

The audit also noted other areas of concern, including management's failure to incorporate security policies and guidance in a timely manner or properly review procedures at the various agency locations.

The IG recommended that the Energy Department address each of the vulnerabilities identified in the report, ensure that development and implementation of cybersecurity policies are in accordance with federal requirements, and strengthen the management review process.

In a written response to the report, Energy Chief Information Officer Thomas Pyke Jr. noted a number of directives the department's cybersecurity team developed to address the various issues noted by IG.