



U.S. Department of Energy
Office of Inspector General
Office of Audits and Inspections

Audit Report

The Department's Configuration Management of Non-Financial Systems



Department of Energy

Washington, DC 20585

February 23, 2012

MEMORANDUM FOR THE CHIEF INFORMATION OFFICER,
CHIEF INFORMATION OFFICER, NATIONAL NUCLEAR
SECURITY ADMINISTRATION, AND
DIRECTOR, OFFICE OF SCIENCE

A handwritten signature in blue ink, appearing to read "Rickey R. Hass".

FROM: Rickey R. Hass
Deputy Inspector General
for Audits and Inspections
Office of Inspector General

SUBJECT: INFORMATION: Audit Report on "The Department's Configuration Management of Non-Financial Systems"

BACKGROUND

The Department of Energy utilizes many types of information technology (IT) systems to support its various missions related to environmental cleanup, national security, energy and scientific research. Protecting these systems has become increasingly challenging as the frequency and sophistication of cyber attacks continues to rise. A key component of helping to ensure an adequate information security posture is the implementation of an effective configuration management program. Configuration management helps to protect the confidentiality, integrity and availability of IT resources through controls over the processes for initializing, changing and monitoring information systems. For instance, active management and testing of configurations is essential for identifying and remediating vulnerabilities in systems and applications. Furthermore, effective use of change controls is integral for managing updates to system configurations and should include proper approvals, testing and validation, and evaluation of security implications of changes.

Prior Office of Inspector General (OIG) reports identified systemic issues with the Department's cyber security and configuration management programs. For instance, our annual evaluation of *The Department's Unclassified Cyber Security Program* identified weaknesses related to configuration management over financial systems for each of the past six years. In light of the need to ensure effective security practices over the Department's information systems and the challenges noted in prior OIG reports, we initiated this audit to determine whether the Department implemented an effective configuration management process over non-financial systems. This review supplements our annual financial statement audit and *Federal Information Security Management Act (FISMA)* evaluation, and focused on non-financial systems and certain sites and observations not included in our other reviews.

CONCLUSIONS AND OBSERVATIONS

We found that the Department had not implemented sufficient controls over its configuration management processes for non-financial systems. The issues we identified were similar to what

we observed with financial systems in our most recent evaluation report of *The Department's Unclassified Cyber Security Program - 2011* (DOE/IG-0856, October 2011). Security patches designed to mitigate system vulnerabilities had not been applied in a timely manner for desktops, applications and servers. In addition, organizations and sites reviewed had not always followed effective procedures to ensure that changes to systems and applications were properly tested and approved prior to implementation.

Vulnerability Management

Although the organizations and sites reviewed had policies and procedures for conducting periodic vulnerability scans of information systems, we found internal vulnerabilities at each location that negatively impacted the security of desktops, non-financial applications, and at two sites, system servers. In addition, we identified external vulnerabilities at one location. External assessments are conducted from outside an organization's security perimeter and offer the ability to view the environment's security posture as it appears from outside the entity with the goal of revealing vulnerabilities that could be exploited by an external attacker. Internal vulnerability assessments assume the identity of a trusted insider or an attacker who has penetrated perimeter defenses. During our internal vulnerability testing, we utilized both authenticated and unauthenticated scanning. Authenticated scanning uses login names and passwords to simulate a user being on the system, while unauthenticated scanning does not use login credentials and typically identifies basic internal network setting vulnerabilities. In particular:

- Scans of desktop machines that could access selected non-financial systems found that 414 of 714 (58 percent) contained vulnerabilities designated as medium or high risk in the National Vulnerability Database, which is sponsored by the Department of Homeland Security. For example, at one Office of Science (Science) site, we found that 56 of 131 (43 percent) desktops contained vulnerabilities. Similarly, 209 of 319 (66 percent) desktops tested at a National Nuclear Security Administration (NNSA) site and all 38 desktops reviewed for one Headquarters organization contained vulnerabilities. We determined that numerous desktops were running programs that were missing security patches or updates that were more than 3 months old. In some instances, patches for identified vulnerabilities had been released by the vendor more than one year prior to our testing. Two organizations and three sites reviewed were also utilizing unpatched versions of office automation software that could have presented the risk that an attacker would be able to execute malicious code or disrupt system operations;
- We identified 14 vulnerabilities at 2 organizations and 3 sites that affected various system applications, including those used to support functions such as procurement and security. Eight of the vulnerabilities were high risk, including at least one that could have been exploited by an attacker to compromise key internal systems and sensitive data. The remaining six weaknesses were medium risk and included vulnerable input validation techniques that could be used by an attacker to obtain unauthorized access to data within the database. Other vulnerabilities identified during our testing of the applications included problems with data protection, access controls, authorization management and

data sanitization – all of which could have allowed a malicious attacker to obtain user credentials, steal sensitive information, or potentially execute malicious programs on the Department's systems;

- At 2 sites, we identified 13 system servers that contained 5 different types of high risk vulnerabilities. Specifically, servers containing potentially sensitive information were missing security patches for various operating systems even though the patches had been released by the vendor more than 30 days prior to our testing. In some instances, patches that had been released by the vendor over two years prior to our testing had not been applied. Absent remediation of the identified weaknesses, the sites were at risk for remote code execution by attackers that could disrupt normal business operations or have negative impacts on system and data reliability; and,
- In addition to the vulnerabilities identified during our internal testing, we also found weaknesses at one site during our external vulnerability assessment. Specifically, we determined that a vulnerability existed on a system in which a remote server could allow anonymous access to the system. This issue could have resulted in the disclosure of information that an attacker could find useful to conduct future exploits. Although officials stated that they had accepted the risk posed by the vulnerability, we found that the acceptance process was informal, lacked a detailed analysis and occurred only after we brought the vulnerability to management's attention during our testing.

The weaknesses described above occurred because procedures were not adequate for identifying and remediating vulnerabilities in a timely manner. For instance, a policy at one site stated that identified high and medium risk vulnerabilities should be remediated within seven days of identification. However, we noted that many of the weaknesses identified were more than three months old because the site's vulnerability scanning process did not include authenticated scans – a key testing method used to identify weaknesses. As such, many of the weaknesses we identified went undetected by the site during its testing. Notably, subsequent to our testing, officials acknowledged that authenticated scanning would be beneficial and commented that they would seek to implement it in the future.

At another site, procedures permitted various amounts of time to pass before vulnerabilities were required to be remediated. Specifically, a scoring process was used to assess the risk of system and vulnerability attributes such as number of missing patches, severity of the patches and the time elapsed since the patches were required. Once the system score reached a certain threshold, the system administrator had seven days to remediate the vulnerability or the system would be blocked from accessing certain network services. While the site stated that it relies on a defense-in-depth approach to cyber security, we found that the procedures described above allowed known vulnerabilities to remain uncorrected on systems for an extended period even when a patch was available.

Without improvements to its vulnerability management program, the Department's desktops, non-financial applications and servers continue to be at risk from internal and external threats. As noted, many of the vulnerabilities we identified created the potential for an attacker to gain unauthorized access to the Department's systems and information.

System Change Controls

Changes to non-financial information systems and applications at six organizations and sites reviewed were not always properly approved, tested or evaluated for security risks prior to their implementation. As noted by the National Institute of Standards and Technology (NIST), an effective change control process is necessary to ensure that only authorized changes are made to systems and that the integrity and security of the system remains intact. In particular, we found:

- The Department had not documented approvals for each configuration change made to the systems reviewed. Specifically, although each of the organizations and sites reviewed had established a process for making changes to information systems, we found that 44 of 197 (22 percent) change requests reviewed did not have documented authorizations indicating that the change had been approved in advance of being initiated. For instance, all 44 change requests reviewed within the Office of the Chief Information Officer (OCIO) lacked documented approvals. Although officials informed us that the proposed changes were reviewed by the OCIO Change Advisory Board, there was no evidence of its decision to accept or deny change requests;
- The Department had not always determined the potential security risks and impacts of system changes prior to actually implementing them. While NIST guidance stressed the need to approve changes to a system with consideration for security implications, we found that the majority of the changes reviewed either did not have a security impact analysis or the analysis was not complete. For example, at Brookhaven National Laboratory (BNL), all 34 changes reviewed were missing documented security impact analyses. In addition, 10 of 44 change requests within OCIO were approved for implementation even though there was no data or inadequate data provided in the "Risk Impact/Assessment" field of the change control form; and,
- Forty-three of 197 (22 percent) changes evaluated did not have test plans and/or test results that analyzed potential functional and security impacts. For example, OCIO had insufficient or no test plans for half of the system changes reviewed. Also, the Los Alamos National Laboratory (LANL) was unable to provide test plans for 10 of the 12 system changes reviewed. In responding to our report, NNSA officials commented that the LANL changes reviewed did not require test plans because the changes were considered "Fast Track" work tickets. However, no information was provided to support this process during our test work, and we found that the system for which the changes occurred did not have a formal change control process in place to describe any such procedures.

The change control weaknesses we identified occurred because procedures were not always adequate for addressing approval, testing or evaluation for security risk prior to implementation. For instance, we noted that while the change control procedures at certain Department organizations addressed the development and execution of testing plans, others did not. In particular, the Configuration Management Plan for Science at Headquarters did not include details or requirements for testing system changes prior to implementation. In addition, BNL officials stated that formalized test plans for system updates and patches were not documented

because the system changes were not complex and were of a routine nature. Furthermore, while certain organizations and sites had established change control guidance, the procedures did not always address the need for a formal security impact analysis. For example, the Office of the Chief Financial Officer's management plan stated that changes were evaluated based on overall impact. While we noted that the impact assessment did address functionality, cost and schedule, it did not include a security analysis. In addition, change control procedures at one organization and one site required a security analysis; however, in many cases, there was no evidence that the analysis was completed even though the changes were approved.

Failure to properly test changes prior to employing them in business or other support systems could have a significant impact on system security, data reliability and system operation. In addition, assessing the potential security impact of system changes is essential to maintaining the security posture and minimizing the risk of a security incident adversely affecting the system.

RECOMMENDATION

As part of our evaluation of *The Department's Unclassified Cyber Security Program – 2011*, which focused primarily on financial systems, we provided a recommendation to develop and implement, as needed, procedures and processes to adequately secure systems and applications. We believe this prior recommendation, once fully implemented, will also help address the adequacy of vulnerability management and change control procedures and processes relating to non-financial systems.

However, during the course of this audit, we identified new configuration management weaknesses that increase the risk of compromise of systems and applications that we reviewed. Detailed information regarding these weaknesses was provided to management at each location where vulnerabilities were identified. We acknowledge that many of the weaknesses we identified may be corrected by the Department if it fully implements the recommendations contained in the above report. Nevertheless, to ensure that the vulnerabilities identified during this review are corrected in a timely manner, we recommend that the Department and NNSA Chief Information Officers work with organizations and sites, as necessary, to correct the specific weaknesses identified in this report.

MANAGEMENT REACTION AND AUDITOR COMMENTS

Department management concurred with the report's recommended action and stated that the issues identified should be corrected during the implementation of planned corrective actions to address our report on *The Department's Unclassified Cyber Security Program – 2011*. In separate comments, NNSA management concurred with the report's recommended action but expressed concern that we did not accurately report that the vulnerabilities identified were found using elevated access privileges. We acknowledge that we were provided with user names and passwords for our internal system work, which was meant to simulate an authenticated system user. As such, the internal vulnerabilities we reported could potentially be exploited by individuals with authenticated credentials. The external vulnerabilities, however, were discovered without the

benefit of elevated privileges and could have been exploited by any external user. Management's comments can be found in Attachment 3.

Attachments

cc: Deputy Secretary
Associate Deputy Secretary
Under Secretary for Nuclear Security
Chief Health, Safety and Security Officer
Chief of Staff

OBJECTIVE, SCOPE AND METHODOLOGY

OBJECTIVE

To determine whether the Department of Energy (Department) implemented an effective configuration management process over non-financial systems.

SCOPE

The audit was performed between November 2010 and February 2012 at Department Headquarters in Washington, DC and Germantown, Maryland; and National Nuclear Security Administration (NNSA) and Under Secretary for Science locations. The audit included internal and external vulnerability scanning conducted by KPMG, LLC on behalf of the Office of Inspector General. Systems we selected for review were unclassified, non-financial systems, categorized as moderate according to the *Federal Information Processing Standards*, and a major application or general support system. We conducted external testing of networks and systems as an outsider without any elevated privileges. We conducted internal system scanning as an authenticated user, that is a user with a valid user name and password, and reported on vulnerabilities that could be exploited by both an insider and a remote attacker. In addition, our work did not include a determination of whether vulnerabilities found were actually exploited and used to circumvent existing controls.

METHODOLOGY

To accomplish our objective, we:

- Reviewed Federal laws and regulations pertaining to information and cyber security such as the *Federal Information Security Management Act of 2002*;
- Reviewed applicable standards and guidance issued by the Office of Management and Budget and the National Institute of Standards and Technology (NIST), such as NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, and the *Consensus Audit Guidelines*;
- Obtained and analyzed documentation from Department organizations and sites pertaining to configuration management programs; and,
- Held discussions with officials from the Department and NNSA.

We conducted this audit in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Accordingly, we assessed significant internal controls and compliance with laws and regulations to the extent necessary to satisfy the audit objective. In particular, we assessed the Department's implementation of the *Government*

Performance and Results Act of 1993 and determined that while it did not have specific performance measures for configuration management, it had established performance measures to improve information technology policy and oversight. Because our review was limited, it would not have necessarily disclosed all internal control deficiencies that may have existed at the time of our audit. We did not solely rely on computer-processed data to satisfy our objective. Computer-assisted audit tools were used to perform probes and scans of various networks and drives. We validated the results of the scans by confirming the weaknesses disclosed with responsible on-site personnel and performed other procedures to satisfy ourselves as to the reliability and competence of the data produced by the tests. In addition, we confirmed the validity of other data, when appropriate, by reviewing supporting source documents.

The Department and NNSA waived an exit conference.

RELATED REPORTS

Office of Inspector General Reports

- Audit Report on [*The Department's Unclassified Cyber Security Program – 2011*](#) (DOE/IG-0856, October 2011). Although positive steps had been taken to address previously identified cyber security weaknesses, additional action was needed to further strengthen the Department of Energy's (Department) unclassified cyber security program and help address threats to its information systems. Weaknesses were found in areas of access controls, vulnerability management, web application integrity, contingency planning, change control and cyber security training. These weaknesses occurred, in part, because the Department had not ensured that cyber security requirements included all necessary elements and were properly implemented; and program elements did not always utilize effective performance monitoring activities to ensure that appropriate security controls were in place.
- Audit Report on [*The Department's Unclassified Cyber Security Program – 2010*](#) (DOE/IG-0843, October 2010). Although corrective actions had been taken to resolve configuration management vulnerabilities identified in our Fiscal Year (FY) 2009 evaluation, weaknesses in these areas persisted. Specifically, problems discovered during the review were attributed to inadequate configuration and vulnerability management controls. Performance testing revealed that all 17 locations reviewed had varying degrees of vulnerable applications on desktop and network systems and devices.
- Audit Report on [*The Department's Unclassified Cyber Security Program – 2009*](#) (DOE/IG-0828, October 2009). Weaknesses with configuration management remained at a number of Department sites. Specifically, weaknesses included software vulnerabilities and deficiencies in implementing common security configurations. Additionally, numerous sites had not implemented the Federal Desktop Core Configurations mandated by the Office of Management and Budget.
- Audit Report on [*The Department's Unclassified Cyber Security Program – 2008*](#) (DOE/IG-0801, September 2008). In regards to configuration management, this report identified weaknesses such as outdated or not appropriately patched software. If software with known vulnerabilities is not updated in a timely manner, the risk that the systems could be compromised increases. Also, a number of Department sites or organizations had not disabled unneeded computer services for their publicly accessible websites. These services increased the risk of malicious damage to these websites. Additionally, the report found that a financial system was not set to log account administrative activity, an essential control which permits management reviews. Furthermore, the report found that certain organizations and sites had not implemented protective measures requiring the adoption of standard desktop configurations and that security controls at another site on computers mostly assigned to foreign nationals from nonsensitive countries were not implemented.

Government Accountability Office Report

- Report on [*Cyber Security – Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems*](#) (GAO-11-463T, March 2011). The U.S. Government Accountability Office (GAO) continued to identify protecting the Federal government's information systems and the Nation's cyber critical infrastructure as a government-wide high risk area. Federal systems continue to be afflicted by persistent information security control weaknesses. For example, as part of its audit of the FY 2010 Financial Statements for the U.S. Government, GAO determined that serious and widespread information security control deficiencies were a government-wide material weakness.


MANAGEMENT COMMENTS



Department of Energy
Washington, DC 20585

January 18, 2012

MEMORANDUM FOR RICKEY R. HASS
DEPUTY INSPECTOR GENERAL
FOR AUDITS AND INSPECTIONS
OFFICE OF INSPECTOR GENERAL

FROM: ROBERT F. BRESE 
DEPUTY CHIEF INFORMATION OFFICER
OFFICE OF THE CHIEF INFORMATION OFFICER

SUBJECT: Comments on the Draft Letter Report on the "Department's
Configuration Management of Non-Financial Systems"

Thank you for the opportunity to review and comment on the subject draft letter report, issued January 9, 2012. The Office of the Chief Information Officer (OCIO), along with the Office of Science, concurs with the report's recommended action. The National Nuclear Security Administration has indicated it would provide comments under a separate cover.

We agree that, as the report stated, the recommendation conveyed as part of the evaluation of *The Department's Unclassified Cyber Security Program 2011* – to develop and implement, as needed, procedures and processes to adequately secure systems and applications – should address the vulnerability management and change control issues identified. The Department previously concurred with that recommendation and its progress towards resolution is being tracked in the Departmental Audit Reporting and Tracking System. Further, as necessary, the OCIO will work with the programs and sites to correct weaknesses where new vulnerabilities were identified.



Printed with soy ink on recycled paper



Department of Energy
National Nuclear Security Administration
Washington, DC 20585

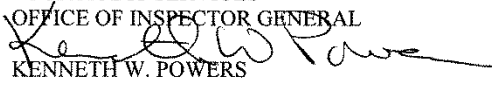


January 31, 2012

MEMORANDUM FOR RICKEY R. HASS

DEPUTY INSPECTOR GENERAL
FOR AUDIT SERVICES
OFFICE OF INSPECTOR GENERAL

FROM:


KENNETH W. POWERS
ASSOCIATE ADMINISTRATOR FOR
MANAGEMENT AND BUDGET

SUBJECT:

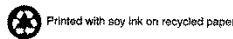
NNSA's Comments on Inspector General Draft Report titled "The Department's Configuration Management of Non-Financial Systems" Project No. A11TG024/IDRMS No. 2010-02345

The National Nuclear Security Administration (NNSA) appreciates the opportunity to review the Inspector General's (IG) draft report, "The Department's Configuration Management of Non-Financial Systems." We understand that this audit was performed as part of and supplemental to the Federal Information Security Management Act (FISMA) evaluation, audit of the Department's unclassified cyber security program for 2011, and annual financial statement audit, focusing on non-financial systems not covered in those reviews. Based on our review, NNSA concurs with the IG findings. Further, as noted in the report, the issues identified should be corrected during the implementation of planned corrective actions to address IG-0856, *The Department's Unclassified Cyber Security Program - 2011*. As such, no corrective actions will be tracked specific to this report, but NNSA will ensure that the more detailed issue descriptions and sites referenced in the report are considered when implementing the corrective actions for IG-0856.

In addition, as previously discussed with the audit staff, the approach for the performed external and internal vulnerability assessments continues to be only partially explained in audit reports of this nature. Specifically, we are consciously allowing the audit team to bypass several layers of controls in order to run their assessments. These layers of controls (perimeter defenses, least privilege, and incident detection and response systems) would preclude the average hacker from being able to exploit a significant number of the vulnerabilities that are being identified in the report. In other words, these assessments are performed with access levels/privileges general users and outsiders don't have. As such, we would request that the final report clearly and prominently caveat that the vulnerabilities were identified using access privileges not afforded to the average user. Therefore, the results should not be construed to indicate the probability or likelihood of these vulnerabilities being exploited under normal circumstances.

If you have any questions concerning this response, please contact Dean Childs, Director, Management Control and Assurance, at 301-903-1341.

Attachment



General Comments:

1. Based on a defense in depth security posture, LLNL takes a risk based approach to the identification and remediation of system vulnerabilities. The report is not accurate as stated in the last paragraph of page 3.

2. Page 3; First bullet; the second sentence of the draft report states: “Specifically, servers containing potentially sensitive information were missing security patches for various operating systems even though the patches had been released by the vendor more than 30 days prior to our testing.”

This sentence should be changed to remove the wording “potentially sensitive information” unless the OIG has specific knowledge of the types of information on these systems. This sentence should be changed to: Specifically, servers were missing security patches for various operating systems even though patches were released by the vendor more than 30 days prior to our testing.

3. Page 3; first sentence; second non-bulleted paragraph of the draft report states: “At another site, procedures permitted various amounts of time to pass before vulnerabilities were required to be remediated.”

This sentence should be changed to: At another site (LLNL), risk based procedures permitted various amounts of time to pass before systems with vulnerabilities are blocked from accessing network services. This process focuses on high risk vulnerabilities and applies a risk based approach to configuration management.

4. Page 3; second sentence; second non-bulleted paragraph of the draft letter report states: “Specifically, a scoring process was used to assess the risk of the system and vulnerability attributes such as number of missing patches, severity of the patches, and the time elapsed since the patches were required.”

This should be changed to: Specifically, a scoring process is used in a risk based approach to assess the risk of the system and vulnerability attributes such as number of missing patches, severity of the patches, and the time elapsed since the patches were required.

5. Page 3; fourth sentence; second non-bulleted paragraph of the draft letter report states: “However, this process could allow known vulnerabilities to remain uncorrected on systems for an extended period even when a patch was available.”

This should be changed to: This process takes a resource impacting and risk based approach and could allow known vulnerabilities to remain uncorrected on systems for an extended period even when a patch was available but the site relies on a defense in depth approach to cyber security.

6. Page 4: third bulleted paragraph of the draft letter report states: *“Also, the Los Alamos National Laboratory was unable to provide test plans for 10 of the 12 system changes reviewed.”*

Auditors asked LANL to provide a specific sample set of change request work tickets. Unfortunately the sample set did not include project work tickets that would have required a test plan. Instead the sample set included maintenance and what LANL terms "Fast Track" work tickets. The Fast Track tickets are used to track normal maintenance activities (e.g. reboot server) and subtasks under bigger scope project/work tickets. LANL reviewed the tickets from sample set that did not have test plans and believes that the work scope for those tickets did not require test plans. Therefore, the audit conclusions are not correct.

LANL requests that the above statement be removed from the audit report. LANL would welcome the opportunity to discuss each of the work tickets and explain why we believe test plans were not required.

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the audit or inspection would have been helpful to the reader in understanding this report?
2. What additional information related to findings and recommendations could have been included in the report to assist management in implementing corrective actions?
3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?
4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?
5. Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact our office at (202) 253-2162.

This page intentionally left blank.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy Office of Inspector General Home Page
<http://energy.gov/ig>

Your comments would be appreciated and can be provided on the Customer Response Form.