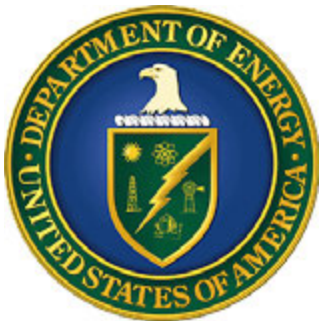

U.S. Department of Energy

Office of Inspector General

Office of Audits and Inspections

AUDIT REPORT

Cybersecurity Controls Over a Major National Nuclear Security Administration Information System

DOE/IG-0938

June 2015

Department of Energy
Washington, DC 20585

June 3, 2015

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Audit Report: "Cybersecurity Controls Over a Major National Nuclear Security Administration Information System"

BACKGROUND

In both the Federal and commercial sectors, cybersecurity is one of the Nation's most pressing concerns. Information system security helps ensure the integrity and safety of system resources and activities. Moreover, as with many private organizations, Federal entities are dependent on the secure operation of their information systems. However, the use of information technology is evolving rapidly and these information systems are exposed to new and constantly changing threats, such as theft, fraud, and abuse.

The National Nuclear Security Administration (NNSA) was established by Congress in 2000 as a semiautonomous agency within the Department of Energy. It is responsible for some of the Department's most sensitive programs, including the management and security of the Nation's nuclear weapons inventory. NNSA's missions require a secure production and laboratory infrastructure meeting immediate and long-term needs. We initiated this audit to determine whether an NNSA information system at one of its key facilities had adequate cybersecurity controls in place. Due to security considerations, the location and system name have been omitted from this report but have been provided to NNSA management.

RESULTS OF AUDIT

Our audit revealed that the system's cybersecurity controls had not been adequately developed, documented, or implemented. Specifically, we identified weaknesses related to the implementation of access controls and the development and implementation of effective database change management, configuration management, and continuous monitoring processes:

- User passwords had not been regularly changed to reduce the risk of system compromise and ensure that users had been authorized to maintain access to the system. Contrary to assertions in the system's risk assessment that certain actions had been taken to mitigate and lower residual risk, we found that the actions had not actually been taken, potentially exposing the system to a higher level of residual risk than reported. In response to our

findings, management indicated that automated password management controls were implemented shortly after our review. However, due to the timing of our fieldwork, we did not verify that corrective actions were in place and operating effectively.

- An effective configuration management process had not been implemented for the system. Vulnerability scans identified a number of devices that had open ports or missing security patches, but management considered the devices low risk as implemented due to the system's physical and logical isolation. However, while the system's isolation reduces the risk of threats posed by outsiders, the open ports and missing patches increased the risk of insider threats to the system—a factor that should have been considered and documented in the system's residual risk assessment.

- The site determined that the system's configuration management process mitigated a number of threats. However, we found that key configuration documentation in the system security plan was, at times, inaccurate and, as a result, unreliable.

- Controls over database change management had not been fully developed or implemented. Specifically, separation of duties and role-based access controls had not been fully implemented. Nor, had a documented change management process for making database modifications been implemented.

- Finally, an effective continuous monitoring program to ensure adequate security over the system was not in place. In particular, annual security control testing, vulnerability scanning, event log reviews, and continuity of operations planning had not been fully implemented.

The weaknesses identified occurred, at least in part, because site officials did not ensure that Federal security requirements were fully implemented to protect the system. Contrary to applicable requirements promulgated by the National Institute of Standards and Technology, the system was put into operation by the site's contractor, as allowed by the site's approved Risk Management Framework, even though various security risks had not been adequately mitigated. In addition, site officials had not established a formal service level agreement with the system's vendor to define ongoing support requirements for the system. As a result, we concluded that the system was at an increased risk of loss of availability and compromise of data integrity. Although we confirmed that compensatory measures were in place to ensure continued security in the event of a system failure, these compensating controls are costly and, if needed, would further strain the site's already limited resources. Most importantly, rarely do compensatory controls serve as a quality substitute for the required controls.

To its credit, after we communicated the issues we discovered to the cognizant NNSA site office, the Authorizing Official withdrew the system's authorization to operate. Further, the operating contractor was directed to perform an in-depth review of the system to ensure that all of the issues described in our report had been appropriately remediated. Such action is encouraging and should enable the site to address the weaknesses cited in our report and each of our specific recommendations.

MANAGEMENT RESPONSE

Management concurred with the report's recommendations and indicated that corrective actions had been initiated or were planned to address the issues identified in the report. Management's comments and our responses are summarized in the body of the report. Management's formal comments are included in their entirety in Appendix 3.

Attachments

cc: Deputy Secretary
Under Secretary for Nuclear Security
Chief of Staff
Chief Information Officer

AUDIT REPORT: CYBERSECURITY CONTROLS OVER A MAJOR NATIONAL NUCLEAR SECURITY ADMINISTRATION INFORMATION SYSTEM

TABLE OF CONTENTS

Audit Report

Appendices

CYBERSECURITY CONTROLS OVER A MAJOR NATIONAL NUCLEAR SECURITY ADMINISTRATION INFORMATION SYSTEM

DETAILS OF FINDING

Cybersecurity controls for the major system reviewed had not been adequately developed, documented, or implemented, resulting in an increased risk to the system's availability and the integrity of the information in the system's database. In particular, we identified weaknesses related to the implementation of access controls and the development and implementation of effective configuration management, database change management, and continuous monitoring processes.

Access Controls

User passwords had not been regularly changed to reduce the risk of system compromise and ensure users had been authorized to maintain access to the system, as required by National Nuclear Security Administration (NNSA) policy. The system's security plan noted that a process was in place to ensure user passwords were changed every 180 days. However, we found that almost half of the system's 116 user account passwords had not been changed within required timeframes. In fact, more than 30 account passwords had not been changed in more than 1 year. In response to our findings, management indicated that automated password management controls were implemented shortly after we reviewed these settings. We did not verify these corrective actions were in place and operating effectively due to the timing of our fieldwork.

In addition, certain controls intended to mitigate threats to the system could not be fully implemented, potentially exposing it to a higher level of residual risk than reported. In particular, the system's residual risk assessment disclosed that vendor default accounts had been removed or default passwords changed to mitigate the threat of improper system use. However, the security plan noted that certain default accounts were still in operation, and passwords could not be changed due to system operation requirements. As such, the ongoing need for these accounts should have been noted and considered in determining whether the weakness had been successfully mitigated to ensure that the system was not susceptible to a higher than reported level of residual risk.

Configuration Management

An effective configuration management process had not been implemented for the NNSA system. Although the system's residual risk assessment disclosed that the implementation of a configuration management process mitigated 6 of the 10 identified threats analyzed, we found that configuration documentation in the security plan was, at times, inaccurate. Configuration management and control processes are an essential part of an effective organization-wide, continuous monitoring program because they provide support in managing, controlling, and documenting changes to a system or its operating environment. We identified discrepancies with certain existing certification documents. For example, the service used to connect remote devices was identified in the configuration baseline as being disabled for a specific router. However, vulnerability scans performed by the site identified that the service was actually running on that component. Management stated that these were services needed for the

application to perform properly. While we agree, this is a deviation from the site's standard configuration that should have been reflected in the component's testing documentation. Such failures to properly document component configurations raise questions regarding the reliability of the system's configuration management process.

In addition, vulnerability scans identified a number of devices that had open ports or missing security patches. The security plan identified some of these devices and disclosed that they were low risk as implemented in the site's environment due to the system's physical and logical isolation. While we agree that system isolation provides some level of security, particularly against outsider threat to the system, enabling unneeded ports and services increases the risk of threats posed by insiders. In addition, this practice conflicts with direction from the National Institute of Standards and Technology (NIST) concerning the implementation of a defense-in-depth information security concept.

Database Change Management

Controls over database change management had not been fully developed or implemented. Specifically, separation of duties and role-based access controls had not been fully implemented on the system. In particular, we found that the system's station designers, system administrators, and system managers—the positions responsible for developing, approving, and activating database changes at the site—each had full system access under all three roles. This bypassed the role-based access control security features highlighted as a mitigating step for a majority of the threats identified in the system's residual risk assessment. Officials stated that the individuals fulfilling these roles had received training and had been instructed not to implement a change independently; however, the ability to do so was present, and our analysis found several cases where the same individual who developed database changes had moved them to the production system. As such, we determined that controls to prevent unauthorized system changes may not have been completely effective.

In addition, the system owner told us that a documented change management process for making database modifications had not been implemented for the system. Instead, officials noted that an undocumented divisional process was in place where users submitted change requests, via email or verbally, through supervisors who would then forward the change to the appropriate personnel. As such, we were unable to confirm that all database changes had been requested, approved, and properly tested prior to implementation. Management stated that the site had limited capability to make changes to the system or its standard suite of services. While we agree that the site cannot make changes to the system's configuration, the maintenance of the underlying database is the sole responsibility of the site.

Continuous Monitoring

Site officials had not implemented an effective continuous monitoring program to ensure adequate security over the system. Specifically, we identified weaknesses related to security testing, vulnerability scanning, audit logging, and contingency planning, leaving the system operating at a higher than necessary risk and more susceptible to loss of availability. In particular, we found the following:

- Annual security control testing was not adequate to ensure controls were in place and effective. Our analysis of the system's security plan found that the vast majority of cybersecurity controls had not been properly documented for implementation or adequately tested. Specifically, we identified issues with 74 percent of the controls in the security plan, including a lack of effective control testing procedures and the failure to address all required control elements. For example, numerous required technical controls were noted as having been tested by confirming the currency of site policies. While we agree it is important that site policies be kept up-to-date, having current policies does not provide assurance that the controls in question had been properly implemented on the system. Although the system's Authorizing Official stated that in-depth testing to support the results noted in the security plan for these controls had been performed, he commented that the procedures conducted had not been fully documented and rendered an independent review of the sufficiency of test procedures difficult. As such, we could not state with certainty that controls had been fully implemented or properly tested. In addition, required control enhancements had been excluded from 43 of the 167 NIST-required control descriptions in the security plan. As a result, these requirements that provide additional protection based on the system's impact level had not been identified for implementation on the system.

- A review of completed vulnerability scans provided by the site determined that not all components within the system had been scanned as required. In particular, the most recent scan results completed by site officials indicated that 28 (42 percent) system components had not been scanned for vulnerabilities, such as missing security patches. In addition, quarterly scans required by the security plan had not always been conducted.

- Event log reviews were not regularly completed even though they were identified as a significant component of the system's continuous monitoring strategy. For example, database changes within the system were only available for review for a limited time after they were activated into production. In addition, the reviews were completed only as needed by the system managers, whose own actions in the system would be under review. Even when log reviews were conducted, the results were not routinely forwarded to appropriate system security officials for independent review. After our review, management indicated that a system administrator had begun conducting daily log reviews. However, we found that these reviews were conducted only twice a week and were performed by an individual that had full system access and the ability to make undetected unauthorized changes.

Officials stated that a robust continuous monitoring process was not needed due to the isolated nature of the system. While not connecting systems to the Internet reduces the risk of threats posed by outsiders, an effective continuous monitoring process can help ensure that the risks from insider threats are minimized.

Federal Security Requirements

The cybersecurity weaknesses identified occurred, in part, because site officials did not ensure that Federal security requirements were fully implemented to protect the system. For example, in accordance with the site's Risk Management Framework approved by the Federal site office, the contractor was permitted to operate the system even though Federal reviews required by NIST were not adequately conducted.

This approval was contingent upon the risk evaluation of the system, completed by the contractor, which resulted in a low residual risk based upon the implementation of mitigating controls. However, NIST Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, required that the Federal Authorizing Official utilize the system authorization package to evaluate and explicitly accept the system's risk prior to it being put into operation. Despite this requirement, we found that the system's low residual risk, as identified by the contractor, was not validated by the Federal Authorizing Official prior to the system being approved and placed into operation. Further, the system was granted approval to operate even though various security risks had not been adequately mitigated. In particular, the system's residual risk assessment—upon which the authorization to operate decision was based—contained numerous mitigation steps that had not been effectively implemented. Despite NIST requirements, the NNSA Risk Management Framework permitted contractor officials to operate the system if all residual risks were determined to be low based on implementation of mitigating controls. However, our review noted that a number of the controls designed to lower the risk were not applicable to the threat identified or were inaccurate or not effective. As such, we concluded that the system's residual risk was understated and that the contractor should have been required to request that the cognizant NNSA site office authorize the system for operation.

Also, contrary to Federal requirements, site officials had not established a formal service level agreement with the vendor to define ongoing support requirements and responsibilities for the system. This led to a misunderstanding by the site of its ongoing system maintenance responsibilities, resulting in cybersecurity weaknesses such as system components with inconsistent security configurations and missing patches. The cognizant NNSA site office completed a review of the security plan in December 2012 and required a number of corrective actions to address weaknesses, including system equipment discrepancies in the security plan and failure to test continuity of operations annually. In addition, it noted that the system was not fully implemented in accordance with its security plan for the site's Risk Management Framework and revealed inattention to detail with regard to the management of a mission-essential cyber system. However, the lack of a service level agreement resulted in significant confusion among officials regarding whether the site or the vendor was responsible for correcting system weaknesses. Notably, the vendor recently identified the lack of service level agreement as a weakness and planned to address it in fiscal year 2015.

System Functionality

While the system's isolation from the site's unclassified network does reduce outsider threats, it does not address the potential risk to the system introduced by granting excessive system

privileges or not establishing a robust change management process. Ultimately, the system's availability is of extreme importance and, although currently unable to be attacked from an external source, an internal attack, improperly secured interconnection, or unintentional mistake could lead to the system not operating as intended or not being available. Therefore, it is important that the system's controls are fully implemented as required.

We confirmed that compensatory measures were in place to ensure continued security in the event of a system failure. However, compensating controls that would be implemented to offset a loss of system availability are costly and would further strain the site's already limited resources. In addition, compensatory controls are not infallible, further supporting the necessity of properly implemented cybersecurity controls.

To its credit, subsequent to receiving our preliminary draft report, the system's Authorizing Official withdrew the authorization to operate and directed the site to perform an in-depth review of the system to ensure that all of the issues described in our report had been appropriately remediated. Although the subsequent report was limited in scope, it did identify issues with communication and definition of roles and responsibilities for operation and management of the system similar to those that we identified. It also recommended that the security plan be updated and the system be fully recertified to ensure that its controls were properly documented and implemented. Such action is encouraging and, when completed, should enable the site to be responsive to our recommendations.

RECOMMENDATIONS

To help strengthen system cybersecurity, we recommend that the Under Secretary for Nuclear Security, in conjunction with the cognizant NNSA site office, direct site management to:

1. Reassess the system's risk assessment to ensure that all mitigating controls are fully implemented and residual risk is appropriately quantified; and

2. Correct, through implementation of appropriate controls, any cybersecurity weaknesses identified in this report.

MANAGEMENT RESPONSE

Management concurred with each of the report's recommendations and indicated that corrective actions had been initiated or were planned to address the identified issues. For instance, management commented that it withdrew the system's authorization for full operations and directed an in-depth reassessment of the system's security posture. Management also stated that it will ensure that actions are taken to support secure operation of the system based on a sound risk assessment prior to recertification and reauthorization.

AUDITOR COMMENTS

Management's comments and planned corrective actions were responsive to our recommendations. Management's comments are included in Appendix 3.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

To determine whether the selected major National Nuclear Security Administration (NNSA) information system had adequate cybersecurity controls in place.

Scope

The audit was performed between June 2013 and May 2015 at an NNSA site. The audit was limited to a review of the cybersecurity controls related to the selected system. Due to the nature of the system and security weaknesses identified, our report omitted the location and name of the information system reviewed. The audit was conducted under Office of Inspector General Project Number A15TG014.

Methodology

To accomplish our objective, we:

- Reviewed applicable cybersecurity laws and regulations;
- Reviewed applicable standards and guidance issued by the National Institute of Standards and Technology;
- Reviewed applicable standards and guidance issued by the Department of Energy and NNSA, as well as prior reports issued by the Office of Inspector General;
- Obtained documentation from and held discussions with officials from the NNSA site, applicable vendor personnel, and the NNSA site office to gain an overall understanding of the selected system and its ongoing requirements;
- Interviewed personnel responsible for maintenance and operation of the selected system; and
- Performed a cybersecurity review of the selected system, to include a review of vulnerability scans conducted by the site.

We conducted this performance 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 objectives. Accordingly, we assessed significant internal controls and the NNSA site's implementation of the GPRA Modernization Act of 2010 and determined that it had established performance measures for cybersecurity. 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 audit objective. We confirmed the validity of data, when appropriate, by reviewing supporting source documents, including the site's vulnerability scans, and confirmed identified weaknesses with responsible on-site personnel.

Management waived an exit conference.

PRIOR REPORTS

- Evaluation Report on *The Department of Energy's Unclassified Cybersecurity Program – 2014* (DOE/IG-0925, October 2014). The evaluation determined that while the Department of Energy (Department) continued to make progress in correcting deficiencies identified in prior years, additional effort was needed to ensure that the risks of operating systems were identified and that systems and information were adequately secured. Specifically, even though contractor resources accounted for a majority of the Department's more than 500 systems, it still had not reported performance metric data for all contractor systems. In addition, the evaluation identified weaknesses in security patch management, system integrity of Web applications, access control, configuration management, and security management. The issues identified occurred, at least in part, because the Department's programs and site reviewed had not ensured that cybersecurity policies and procedures were developed and properly implemented. In addition, the Department's performance monitoring and risk management programs were not completely effective. Without improvements, the Department's unclassified cybersecurity program will continue to operate at a higher-than-necessary level of risk.

- Audit Report on the *Management of Naval Reactors' Cyber Security Program* (DOE/IG-0884, April 2013). The audit identified weaknesses related to vulnerability management, access controls, incident response, and security awareness training that could negatively affect its security posture. In particular, the Naval Reactors' vulnerability management controls and processes were not fully effective in applying security patches for all desktop and network applications. In addition, controls over access to information and systems at Naval Reactors were not always operating effectively. Also, our review identified that a confirmed cybersecurity incident involving malicious code located on the unclassified network in January 2012 was not reported to the Department's Joint Cybersecurity Coordination Center, as required. Furthermore, although Naval Reactors had established a cybersecurity awareness training program, its implementation was not always effective. The weaknesses identified occurred, in part, because Naval Reactors had not ensured that necessary cybersecurity controls were fully implemented. In addition, Naval Reactors had not always effectively utilized Plans of Action and Milestones to track, prioritize, and remediate cybersecurity weaknesses. Absent a fully effective cybersecurity program, information systems and data remain at a higher-than- necessary risk of compromise.

- Audit Report on *Management of Los Alamos National Laboratory's Cyber Security Program* (DOE/IG-0880, February 2013). The audit identified continued concerns related to Los Alamos National Laboratory's (LANL) implementation of risk management, system security testing, and vulnerability management practices. In particular, LANL had not always developed and implemented an effective risk management process consistent with Federal requirements; ensured that it had developed, tested and implemented adequate controls over its information systems; and had not always properly addressed critical high-risk vulnerabilities. The issues identified occurred, in part, because of a lack of effective monitoring and oversight of

LANL's cybersecurity program by the Los Alamos Site Office, including approval of practice that were less rigorous than those required by Federal directives. In addition, the audit found that LANL's Information Technology Directorate had not followed National Nuclear Security Administration policies and guidance for assessing system risk and had not fully implemented LANL's own policy related to ensuring that scanning was conducted to identify and mitigate security vulnerabilities in a timely manner.

MANAGEMENT COMMENTS

Department of Energy
Under Secretary for Nuclear Security
Administrator, National Nuclear Security Administration
Washington, DC 20585

April 22, 2015

MEMORANDUM FOR GREGORY H. FRIEDMAN
INSPECTOR GENERAL

FROM: FRANK G. KLOTZ FK 4/22/2015

SUBJECT: Comments on the Office of Inspector General Draft Report Titled Cybersecurity Controls Over a Major National Nuclear Security Administration System (A15TG014/2012-03268)

Thank you for the opportunity to review and comment on the subject draft report. The National Nuclear Security Administration (NNSA) concurs with the recommendations to reevaluate the system's risk and correct issues identified by the auditors. As noted in the report, upon discovery of these issues, NNSA immediately withdrew the system's authorization for full operations and directed an in-depth reassessment of its security risk posture.

The reassessment report was completed in September 2014. Detailed corrective actions are in process to support recertification and resumption of full system operations. We anticipate all actions to be completed and validated by June 30, 2015.

The attachment to this memorandum provides the response to each recommendation along with timelines for completion. We have also provided technical comments under separate cover for your consideration to enhance the clarity and accuracy of the report. If you have any questions regarding this response, please contact Dean Childs, Director, Audit Coordination and Internal Affairs at (301) 903-1341.

Attachment

Response to Report Recommendations
Cybersecurity Controls Over a Major
National Nuclear Security Administration System

Recommendation 1: Reassess the system's risk assessment to ensure that all mitigating controls are fully implemented and residual risk is appropriately quantified.

Management Response: ***Concur***

On August 14, 2014, the cognizant field office formally withdrew the system's authorization for full operations and directed an in-depth reassessment of the system's security risk posture. The self-assessment report was completed on September 12, 2014. NNSA is continuing to monitor and evaluate on-going corrective actions to ensure risks have been adequately identified and mitigated prior to making a decision to reauthorize full system operations. The estimated completion date for these activities is June 30, 2015.

Recommendation 2: Correct the cybersecurity weaknesses identified in this report through implementation of appropriate controls.

Management Response: ***Concur***

NNSA will ensure all appropriate corrective actions are taken to support secure operation of the system based on a sound risk assessment prior to recertification and reauthorization. This will include actions to address issues identified in the final Inspector General report as appropriate. The estimated completion date for these activities is June 30, 2015.

FEEDBACK

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We aim to make our reports as responsive as possible and ask you to consider sharing your thoughts with us.

Please send your comments, suggestions, and feedback to OIG.Reports@hq.doe.gov and include your name, contact information and the report number. Comments may also be mailed to:

Office of Inspector General (IG-12)
Department of Energy
Washington, DC 20585

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