U.S. Department of Energy

Office of Inspector General

Office of Audits and Inspections

AUDIT REPORT

The Department of Energy's Cybersecurity Risk Management Framework

DOE-OIG-16-02

November 2015

Department of Energy
Washington, DC 20585

November 4, 2015

MEMORANDUM FOR THE SECRETARY

FROM: Rickey R. Hass
Acting Inspector General

SUBJECT: INFORMATION: Audit Report: "The Department of Energy's Cybersecurity Risk Management Framework"

BACKGROUND

Cyber attacks on information systems have become aggressive, disciplined, well-organized, and very sophisticated. The threat environment also continues to change and become more complex. In response, the Department of Energy began transitioning several years ago from a compliance-based information system certification and accreditation process to a cybersecurity risk management framework. This change was designed to allow the Department to more effectively manage the risks to its information systems and retain assurance that new risks are identified and mitigated in a timely manner. Through this risk-based process, the Department is moving toward continuous system authorizations, which decreases the burden on cybersecurity resources. In addition, it allows the frequency of testing, as well as the necessary resources, to be balanced with the level of risk that systems introduce to the processing environment.

In fiscal year 2015, the Department planned to spend at least $300 million on cybersecurity activities designed to protect information technology resources supporting its national security, energy, science, and environmental missions. Prior Office of Inspector General audits and evaluations have indicated the need for improvements to the Department's cybersecurity program in the areas of patch management, configuration management, and control testing. In light of the current transition to a continuous risk-based cybersecurity management process, we initiated this audit to determine whether the Department had effectively implemented its cybersecurity risk management framework.

RESULTS OF AUDIT

The Department had made progress toward implementing an unclassified cybersecurity risk management framework designed to reduce the likelihood of compromise to its information systems and data. For instance, the Department implemented the use of a software application to better analyze system risks, and at least one site reviewed had developed a tracking system to enhance communication with its authorizing official, the Federal official responsible for accepting risks and approving an information system for operation. However, we found that additional effort is needed to ensure that operating system risks are identified and systems and

information are adequately secured. For example, programs and sites had not always properly categorized the risk to systems or implemented appropriate security controls. Although certain controls had been established, officials had not always thoroughly and independently assessed or monitored such controls to ensure they were effective. Further, programs and sites had not ensured that authorizing officials responsible for accepting system risk were fully aware of the risks, weaknesses, and vulnerabilities to the information systems under their purview. Specifically, our review of 25 systems at 6 sites found that Federal and/or contractor officials had not always done the following:

- Properly categorized unclassified information systems to reflect the appropriate impact level for the loss of the confidentiality, integrity, and availability of the information contained within those systems. We identified one system at a National Nuclear Security Administration site that was not assigned the appropriate system risk categorization and related controls despite the severe impact to organizational operations that could occur if the system was not available.

- Selected and implemented the appropriate controls necessary for protecting information systems and data from potential loss or unauthorized disclosure. For example, system security plans across various programs did not provide adequate details related to how required security controls were implemented or included contradictory information about how controls were applied. Officials also had not always appropriately assessed controls for effectiveness. For instance, Brookhaven National Laboratory had not thoroughly tested security control implementation on any of the three systems selected for review.

- Ensured that authorizing officials were fully aware of the risks and weaknesses present on the information systems under their purview. Even though required by Federal cybersecurity standards, none of the sites reviewed had provided authorizing officials with all pertinent and known risk information. As an example, Federal officials at the National Renewable Energy Laboratory did not review a system's risks to determine if they were acceptable until 4 years after placing the system in operation.

- Fully developed and implemented continuous monitoring programs to help retain ongoing assurance that risks are appropriately managed. Continuous monitoring supports the initial authorization process through reporting of pertinent cybersecurity information including assessment data pertaining to, and metrics data obtained from, system-level security controls. However, we found that a process for identifying useful metrics for cybersecurity monitoring had not been developed, system log reviews were not conducted as appropriate, and activities in plans of action and milestones were not fully implemented in a timely manner.

The weaknesses identified existed, in part, because Federal requirements for securing information systems had not been fully implemented, and the Department had not established sufficient oversight and communication to support its cybersecurity risk management program. Specifically, key aspects of a successful risk management program were not developed or maintained. For example, policies and procedures were not updated to account for changes in risk management requirements, and control effectiveness was not validated against Federal

requirements and best practices. In addition, Federal officials had not provided adequate oversight to ensure effective risk management practices had been implemented. For instance, we found that Federal officials may have prematurely approved one site's transition to a continuous authorization process even though the necessary resources were not in place to support such a change. Furthermore, Department management had not always ensured that risk tolerances were established and communicated to field elements as required to help ensure the implementation of an effective risk management program.

Notably, Oak Ridge National Laboratory implemented an automated process for identifying system vulnerabilities, assigning work orders, and tracking the progress through resolution to aid its risk management process. In addition, the Office of Environmental Management had developed a robust continuous monitoring capability to centrally monitor system and network performance at most of its locations. Furthermore, subsequent to our fieldwork, the authorizing official for the Y-12 National Security Complex revoked the site contractor's approved risk management framework after it operated information systems outside of the established process. While these are positive actions, additional effort is needed across the Department. Without improvements to its cybersecurity risk management program, the Department cannot ensure that it has an ongoing understanding of the risks to its systems and to what extent those risks have been or can be mitigated. As a result, risk acceptance decisions may be based on inaccurate information, and the Department's systems and information may be placed at an increased risk of compromise. Therefore, we made recommendations that, when fully implemented, should help improve the Department's cybersecurity risk management framework.

MANAGEMENT RESPONSE

Management generally concurred with the recommendations and indicated that corrective actions had been initiated or were planned to address most of 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
Administrator, National Nuclear Security Administration
Chief of Staff
Chief Financial Officer

AUDIT REPORT: THE DEPARTMENT OF ENERGY'S CYBERSECURITY RISK MANAGEMENT FRAMEWORK

TABLE OF CONTENTS

Audit Report

Appendices

THE DEPARTMENT OF ENERGY'S CYBERSECURITY RISK MANAGEMENT FRAMEWORK

DETAILS OF FINDING

In 2011, the Department of Energy (Department) began transitioning from a cyclical, compliance-based information system certification and accreditation process to a cybersecurity risk management framework (RMF). An effective RMF is designed to manage information systems in an ever-changing and increasingly complex threat environment by measuring security control implementation and the residual risks to those systems on a continuous basis. In addition, an RMF enables an organization to move to a continuous risk-based system authorization process, which is intended to lessen the burden on resources and balance the frequency and resources needed for testing and reviewing controls. To enable implementation of an RMF, the National Institute of Standards and Technology (NIST) developed a six-step process for agencies that involves continually reviewing and improving a system's security posture on a more ongoing basis than had previously occurred.

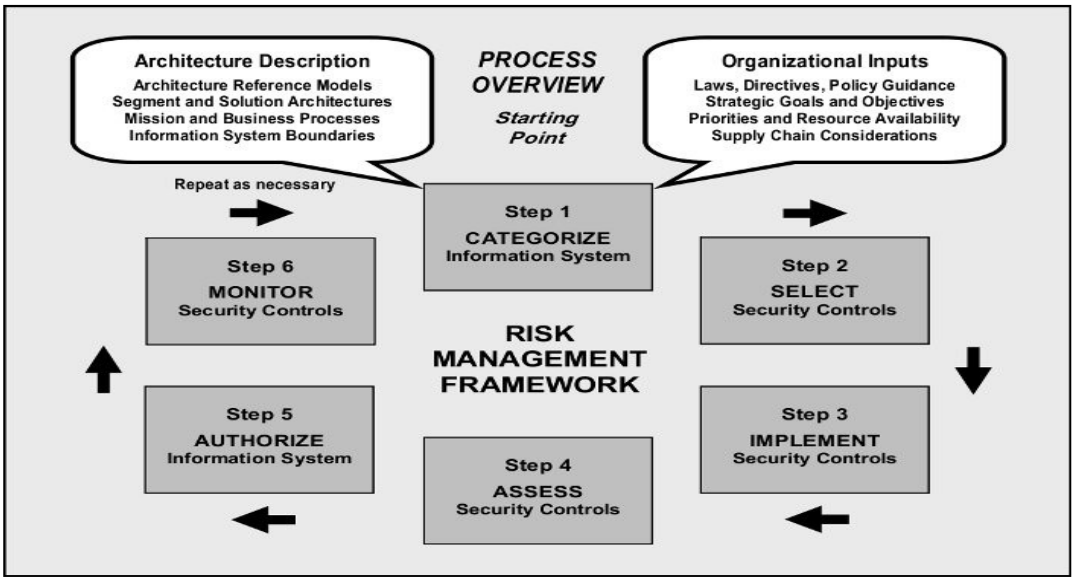

Figure 1: Risk Management Framework[1]

The Department had made progress towards implementing an unclassified cybersecurity RMF designed to reduce the likelihood of compromise to its information systems and data. For instance, the Department had implemented the use of a software application to better analyze system risks, and at least one site reviewed had developed a tracking procedure to enhance communication with its authorizing official.[2] However, we found that the Department had not fully implemented a cybersecurity RMF over unclassified information systems to reduce the likelihood of compromise to its systems and/or the data they contained. Specifically, programs and sites had not always properly categorized the impact to systems or selected and implemented appropriate security controls based on the assessed impact level. In addition, although certain

[1] Source: National Institute of Standards and Technology Special Publication 800-37, Revision 1.
[2] An Authorizing Official is a senior Federal official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk.

controls had been established, officials had not adequately assessed or monitored controls to ensure that such controls were effective. Further, programs and sites had not ensured that authorizing officials responsible for accepting system risk were fully aware of the risks and weaknesses affecting the information systems under their purview.

System Categorization

One of six sites reviewed—a National Nuclear Security Administration (NNSA) site—had not always categorized unclassified information systems to properly reflect the potential impact (assessed as high, moderate, or low) of a loss in confidentiality, integrity, or availability. [3] Accurately categorizing an information system is a critical initial step of an effective RMF. Failing to do so can result in under-protecting the system by not implementing all appropriate controls. This could place important assets and sensitive data at increased risk of unnecessary loss or disclosure, potentially impairing the Department's ability to accomplish its mission. To that end, NIST established specific Federal requirements to be used by agencies when categorizing information systems.

Contrary to those requirements, 1 of the 8 systems we reviewed at the NNSA site had not been properly categorized. Specifically, the site did not properly categorize a supervisory control and data acquisition system used for managing electricity. Due to its critical nature, this system required constant availability and directly affected mission requirements but was categorized as moderate, rather than high. NIST's *Guide to Industrial Control Systems (ICS) Security* and its *Guide for Mapping Types of Information and Information Systems to Security Categories* required such systems to be categorized as high impact systems because of the potential catastrophic loss of system availability, including costs to replace the system and the aggregated effect such loss could have on the mission. However, several controls related to areas such as accessibility, system and information integrity, and configuration management had not been selected for implementation, controls essential to adequately protecting the Department's assets and information. As noted by Federal requirements, proper categorization of systems is essential to ensuring that all necessary controls are implemented.

Control Implementation and Assessment

Programs and sites had not always selected and implemented required cybersecurity controls necessary for protecting information systems and data from potential loss or unauthorized disclosure. In addition, programs and sites had not appropriately assessed controls for effectiveness. As the Department transitions from the static certification and accreditation process toward continuous authorization for its information systems, it is important that programs and sites use robust control testing protocols to understand the risks that may affect systems and whether such risks should be accepted.

[3] According to Federal Information Processing Standard 199, confidentiality preserves authorized restrictions on information access and disclosure, integrity guards against improper information modification or destruction, and availability ensures timely and reliable access to and use of information.

Headquarters and site officials had not always selected and implemented the appropriate controls for minimizing risk to the information technology environment and systems. For example, we found the following:

- Y-12 National Security Complex (Y-12) officials had not documented the implementation of approximately 40 percent of the more than 150 required controls for 2 moderate impact systems reviewed. As such, site officials were unable to provide adequate assurance that these controls had been addressed. A third major system utilized controls based on an outdated version of NNSA policy and did not have documentation supporting the implementation of any required NIST controls. In addition, the authorizing official for Y-12 indicated that all security controls for the site's systems were tested annually. However, our review of the most recent test results found they had not addressed all required NIST controls.

- The Oak Ridge National Laboratory had not fully documented the implementation of controls related to areas such as access control, configuration management, and contingency planning in its common control catalog used as a security baseline for all systems at the site. In many instances, individual system security plans and other documentation did not provide additional details related to the implementation of these controls, measures that could have bolstered the security posture of the systems.

- The 25 system security plans reviewed did not always identify or match how controls were actually implemented. For example, one NNSA site modified the implementation of a security control for a system following a successful attack. However, the system's security plan had not been updated to reflect the new implementation, and the authorizing official had not been notified of the change. Although the modification increased user accessibility, we determined that it weakened the overall effectiveness of the control, potentially increasing the likelihood of system compromise.

Even when controls were appropriately selected, testing was not always adequate. We found that Brookhaven National Laboratory (BNL) had not thoroughly tested security control implementation on any of the three systems we selected for review. As a result, the authorizing official did not have assurance that control test results were valid and could be used to make credible, risk-based decisions. In addition, contrary to Federal requirements emphasizing the need for independence when evaluating security controls, we noted that cybersecurity officials at BNL were responsible for both implementing certain controls and testing their effectiveness. NIST requires that security control testing be conducted by assessors that are free from any actual or perceived conflicts of interest with respect to the development, operation, and/or management of the information system being tested. Furthermore, officials at several sites noted that they utilized reviews performed by the Office of Inspector General, U.S. Government Accountability Office, and the Department's Office of Enterprise Assessments to help meet annual security control assessment requirements. While we agree that these assessments provide the required independence, they are designed to provide oversight over the Department's cybersecurity processes and procedures and should not be relied upon as a substitute for

comprehensive, independent testing of security controls. Specifically, these assessments may not have been conducted at a level of granularity that would provide sufficient evaluation of cybersecurity controls at the system level.

Further, system control tests at multiple sites reviewed did not provide meaningful assurance that a control had been effectively implemented to minimize risk to the information system. Specifically, tests performed did not always align with the control objective, and technical controls often relied upon a review of policy or interviews rather than performance of more substantial procedures. For example, at one site, a control designed to ensure the system owner reviewed physical and logical access authorizations for transferred personnel was determined to be sufficient based on an interview with the official rather than a review of a sample of authorizations to ensure appropriate approvals were obtained. In addition, at least two sites had not thoroughly defined control testing criteria. For example, Lawrence Livermore National Laboratory relied upon the use of "good" software engineering standards as evidence that controls were implemented effectively but did not define how such standards were determined.

System Authorization

None of the locations reviewed had ensured that authorizing officials were fully aware of the risks and weaknesses present on the information systems under their purview. Even though NIST required that the authorizing official explicitly accept known risks to the system that were not mitigated, none of the sites reviewed had provided authorizing officials with all pertinent and known risk information. For example, certain risks identified during testing for a Headquarters system were not presented to the authorizing official because system operators deemed that the risks were unimportant. In addition, a weakness that had been previously accepted as a risk was not included in the results of annual testing even though it had not been mitigated. Therefore, the weakness may have appeared to the authorizing official as having been mitigated when it had not. In another instance, officials at an Office of Energy Efficiency and Renewable Energy location did not review a system's risks to determine if they were acceptable until 4 years after placing the system into operation. Similar findings were identified in our special report on the *Office of Energy Efficiency and Renewable Energy's Integrated Resource and Information System* (DOE/IG-0905, April 2014).

Lawrence Livermore National Laboratory had not always informed its authorizing official of security significant events affecting one of the systems we reviewed. Specifically, the site's approved RMF did not consider downgrades to a system's risk rating as security significant. As such, the site contractor lowered the security risk categorization for an existing system without approval from the authorizing official. Both contractor and Federal officials at the site stated that lowering the rating level would indicate a lower amount of risk. However, NIST defined a significant change as one that is likely to affect the security state of an information system either positively or negatively, including modifications to the security controls. Notably, Lawrence Livermore National Laboratory had developed a tracking system to identify what information had been shared for authorizing official approval.

Also, at the time of our audit, the Y-12 authorizing official had accepted the risk of operating the site's systems prior to all risks being fully identified. We noted that the site's approved risk

management approach allowed it to operate unclassified systems without formally consulting the authorizing official if residual risks could be mitigated to a low level. As such, the authorizing official may not have been aware of risks and did not explicitly accept system risks prior to authorization, as required. NIST requirements noted that the authorizing official should maintain sufficient knowledge of an information system's security state for determining risk acceptance. Following the completion of our fieldwork at Y-12, the authorizing official revoked approval of the site contractor's risk management approach after the contractor operated information systems outside authorized parameters. Until the authorizing official's decision is reversed, the practice of operating systems without explicit approval if residual risks are mitigated to a low level is not permitted.

Continuous Monitoring

The Department had not fully developed and implemented continuous monitoring programs to help retain ongoing assurance that risks were appropriately managed. Continuous monitoring supports the initial system authorization process through the reporting of pertinent cybersecurity information including assessment data pertaining to and metrics obtained from system-level security controls. This process can include aspects such as performance metrics, log reviews, and network monitoring. We also found the following:

- At the six sites reviewed, the process for maintaining useful metrics for monitoring and prioritizing cybersecurity issues had not been fully developed to support ongoing authorization decisions. For example, BNL had not implemented a process to fully develop cybersecurity metrics for its systems related to common control testing and remediation of vulnerabilities that could have supported an effective continuous monitoring approach. In addition, although a Headquarters office had created dashboards for understanding current risks and vulnerabilities, they were populated with data that had not been validated and could provide misleading results. We recognize that developing and maintaining metrics is an ongoing effort that requires attention and action as security risks evolve. However, none of the sites reviewed had developed a formal process for periodically assessing and updating cybersecurity metrics as operating and risk environments changed to ensure they continued to provide meaningful information to risk acceptance officials.

- System log reviews often occurred as a result of an event rather than as a tool for proactively and continuously monitoring control effectiveness. Contrary to NIST requirements, two sites reviewed had not implemented automated log reviews for moderate impact systems. Automated reviews could improve the Department's ability to determine whether previously existing but unknown risks had already affected an information system. At the time of our review, the Department had begun making improvements to support automating system log reviews, but this effort had not been completed. While manual retroactive log reviews were conducted in many cases, this type of review is labor intensive, exhausts limited resources, and is generally less effective. Notably, the Lawrence Livermore National Laboratory had developed a centralized, automated log review process that included retroactive reviews.

- Although plans of action and milestones (POA&Ms) were typically developed to support continuous monitoring, corrective actions were not always implemented in a timely manner. For example, more than 2 years after a POA&M had been created, officials had still not implemented a number of controls for a Headquarters system, including automated mechanisms to audit account creation, modification, and disabling of individual accounts. Similar weaknesses were also identified at other locations. Findings related to POA&Ms have been noted in other Office of Inspector General reports, including *The Department of Energy's Unclassified Cybersecurity Program – 2014* (DOE/IG-0925, October 2014). While programs and sites may have legitimate reasons for milestones exceeding expectations, POA&Ms are used by the Department and the Office of Management and Budget to promote greater attention to security as a fundamental management priority and assist in the budget process.

Absent an effective continuous monitoring process to support ongoing system accreditations, there is limited assurance that controls will remain in place and will continue operating effectively. As such, remediation of the issues identified above is essential to helping ensure that the Department can effectively move to a risk-based cybersecurity management approach.

Cybersecurity Requirements, Oversight, and Communication

The weaknesses identified existed, in part, because Federal requirements and best practices for securing information systems had not been fully implemented. In addition, officials at the programs and sites reviewed had not always provided effective monitoring and oversight of security activities or communicated important risk management information to the appropriate individuals.

Federal Requirements and Best Practices

The Department had not ensured that policies and procedures were developed and implemented in accordance with Federal requirements. Specifically, Department Order 205.1B, *Department of Energy Cyber Security Program*, which served as the baseline for its individual elements' cybersecurity programs, inappropriately required controls from a specific version of NIST to be implemented. Under the current risk-based cybersecurity framework that encourages the implementation of continuous system authorization coupled with a rapidly evolving threat environment, it is important that programs and sites have the ability to implement controls without waiting for detailed policy updates. However, we found that although agencies were required to comply with revised NIST publications within 1 year of the release date, sites had not formally considered many newer controls in a timely manner because of the Department's overly prescriptive directive.

The Department's programs and sites also had not always updated cybersecurity program documentation in a timely manner. For example, the program cybersecurity plan for the Office of Science (Science) had not been updated since June 2010 despite the plan noting it would be reviewed biennially and updated as needed to address new cybersecurity risks or changes to Federal or Department policy. As such, a formal process had not been established for its sites to transition to a risk-based cybersecurity program. Furthermore, Y-12 had not updated its system

security plans to incorporate NNSA cybersecurity requirements established over 2 years ago, even though NNSA Headquarters officials commented that implementation should normally occur within 12 to 18 months. Had the Department and NNSA better enabled their sites to more quickly implement new requirements, the weaknesses identified related to the failure to implement newer controls may have been avoided. Notably, the Office of Environmental Management had incorporated the most recent NIST control baselines into its risk management program, and the Office of the Chief Financial Officer had begun testing controls against updated baselines.

We also found that contrary to Federal requirements, the Department had not fully developed and/or approved continuous monitoring plans, which are key drivers for continued system authorization and measuring the overall effectiveness of system security. NIST Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, states that a robust continuous monitoring plan provides organizations with information necessary to support risk response decisions, security status information, and ongoing insight into security control effectiveness. However, the six locations reviewed had not fully developed continuous monitoring plans to better assist in making effective risk management decisions.

Even when policies were developed, they were not always implemented in accordance with requirements. In particular, an NNSA site had not always accurately categorized systems and obtained the authorizing official's approval for system operation. For example, contrary to Federal requirements, the site continued to categorize the impact of the loss of availability for one of its systems as moderate despite the critical nature and potential severe adverse effect the loss could have on organizational operations. In addition, although NIST required new authorizing officials to review current authorization decisions to determine whether he or she was willing to accept the currently documented risk, we noted that two Headquarters authorizing officials had assumed responsibility over systems without evaluating whether risks continued to be acceptable.

Oversight and Communication

Federal officials may have prematurely approved the sites' transition to a continuous authorization process even though continuous monitoring processes were not in place or fully developed to support such a change. Specifically, we identified a lack of control testing and monitoring at several sites. For instance, we found that although BNL had identified weaknesses regarding performing ongoing control testing, replacing departed cybersecurity staff, and providing training to maintain and develop existing staff, Federal officials approved the transition to a continuous authorization process without assurances that the identified weaknesses would be remediated. Brookhaven Site Office officials noted that since our visit, BNL had been actively working to complete control testing and was in the process of implementing an ongoing, periodic control testing program to identify weaknesses.

Although several authorizing officials and system owners indicated they placed a high level of reliance on mitigating the weaknesses identified in POA&Ms, we found that problems continued to exist in the Department's process. For example, 9 months prior to our review, the

Department's Office of Enterprise Assessments identified that an Office of Energy Efficiency and Renewable Energy site did not monitor internal network traffic. Despite the possibility that weaknesses related to a lack of monitoring could allow malicious activity to go undetected, a POA&M had not been developed, and the weakness continued. Prior Office of Inspector General reviews have consistently noted problems with the Department's POA&Ms not including known weaknesses, missing milestone completion dates, and having unreliable values assigned to mitigate each weakness. Improvements to the POA&M process could assist management in prioritizing its cybersecurity activities and enhancing the risk management process.

We also found that Department management had not always ensured that risk tolerances were established and communicated to field elements, as required. Although NNSA had developed an overall risk statement that Headquarters and field sites could build upon, other programs had neither identified what was an acceptable level of risk nor developed a process for aggregating risk at the site, program, or Department level. While assessing the level of acceptable risk may occur on a case-by-case basis for system authorization purposes, NIST stated that defining an organizational risk tolerance is fundamental to the effectiveness of a risk management program by placing constraints on how much risk is appropriate. Also, recent industry studies indicated that defining and communicating acceptable levels of risk at all levels, including a specific level of risk tolerance, was a best practice for implementing an RMF. While each program, site, and information system may have unique characteristics, understanding how risk acceptance at each level affects the Department as a whole could minimize the effects of a successful compromise. For example, many of the inherited risks associated with Headquarters hosted systems had not been communicated to authorizing officials for those systems even though this issue had been identified in the aftermath of a significant security breach in July 2013.

Opportunities for Improvement

Without improvement to its cybersecurity risk management program through implementation of current Federal requirements and improved oversight and communications, the Department cannot ensure that it has a complete understanding of the risks to its systems and to what extent they can be mitigated. As a result, risk acceptance decisions may be based on inaccurate information, and the Department's systems and information may be unnecessarily placed at an increased risk of compromise. Such compromises can negatively affect the Department's ability to apply resources for defending against cyberattacks. For example, the July 2013 breach alone cost the Department approximately $3.7 million in lost labor hours and funds expended that could have been better used advancing the Department's risk-based cybersecurity framework.

In addition, the cybersecurity risk management process, as implemented, did not provide the level of assurance necessary to support continuous system authorizations, as encouraged by NIST. Implementing the recommendations from this report should improve the Department's cybersecurity risk management program as it continues to move toward continuous authorization of its information systems. Successful transition will depend on the RMF being effectively applied across the Department, to include a robust continuous monitoring program. These

elements are necessary to ensure system owners and authorizing officials can be provided a near real-time view of the security and risk posture for their operating environment and information systems.

RECOMMENDATIONS

To improve cybersecurity risk management practices, we recommend that the Administrator for the National Nuclear Security Administration, Under Secretary for Science and Energy, and Deputy Under Secretary for Management and Performance, in coordination with the Chief Information Officer, as appropriate:

1. Develop, implement, and maintain Department, program, and site level cybersecurity policies and procedures that are consistent with current Federal requirements and best practices.

2. Develop and implement effective oversight and communication of cybersecurity risk management practices by:

    a. Ensuring that continuous authorization processes are approved only when they can be adequately supported and sufficiently resourced;

    b. Ensuring that POA&M processes are complete and effectively implemented; and

    c. Establishing and communicating risk tolerance levels for Department elements, as appropriate, and consistently relaying all known weaknesses to risk acceptance officials.

MANAGEMENT RESPONSE

Management generally concurred with the recommendations. NNSA only partially concurred with the first recommendation and indicated that it did not agree that our findings were due, in part, to a lack of Department or program policy. Rather, NNSA asserted that problems occurred with the application of existing policies and procedures. In addition, Science partially concurred with the second recommendation and suggested that sufficient resources were only one element of a successful continuous authorization program.

Management indicated that corrective actions had been initiated or were planned to address the issues identified in the report. For example, the Office of the Chief Information Officer noted that the Department planned to update its cybersecurity order to support NIST's cybersecurity risk management framework and include Federal requirements and best practices. In addition, Science planned to develop and promulgate risk tolerance levels and site requirements for the development, implementation, and maintenance of continuous monitoring and authorization for its information systems. Also, NNSA committed to extending continuous monitoring using its automated system to support continuous authorization efforts. The Office of Energy Efficiency and Renewable Energy indicated that a contractor assurance system was in development at the National Renewable Energy Laboratory that would align with the Department's risk management framework.

AUDITOR COMMENTS

Management's comments and planned corrective actions were generally responsive to our recommendations. Although management commented that weaknesses were not due to issues with the Department's policy, we noted that the Department's cybersecurity directive prescribed an outdated version of Federal requirements. As noted in our report, enhancements to the cybersecurity policy could enable programs and sites to implement controls without waiting for detailed policy updates from the Department.

In addition, implementation of the second recommendation by all programs should assist the Department in improving oversight and communication of cybersecurity risk management practices as its information systems are transitioned to a continuous authorization approach. Specifically, the Department's programs and sites should ensure that a robust cybersecurity risk management program that includes a fully developed continuous monitoring capability has been implemented prior to allowing systems to continually operate. Providing adequate support and sufficient resources are necessary for the entire cybersecurity risk management program, not just those activities related to system authorization. Management's comments are included in Appendix 3.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

To determine whether the Department of Energy (Department) cybersecurity risk management framework was effectively implemented.

Scope

This audit was performed between June 2014 and November 2015 at Department Headquarters in Washington, DC, and Germantown, Maryland; Lawrence Livermore National Laboratory in Livermore, California; National Renewable Energy Laboratory in Golden, Colorado; Brookhaven National Laboratory in Upton, New York; and Y-12 National Security Complex and Oak Ridge National Laboratory in Oak Ridge, Tennessee. This audit was conducted under Office of Inspector General project number A14TG041.

For our review, we used the National Institute of Standards and Technology (NIST) definition of cybersecurity risk management framework. Specifically, NIST developed an overarching framework for agencies to use when developing a risk-based framework. This practice consists of a six-step process for continually reviewing and improving a system's security posture including categorizing information systems; selecting, implementing, and assessing security controls; authorizing information systems; and monitoring security controls. Our review was limited to unclassified information systems.

Methodology

To accomplish the audit objective, we judgmentally selected a sample of six Department locations, including Headquarters, at which to conduct test work. This selection was based on information obtained during interviews with Headquarters, budgetary figures, and prior audit work. Additionally, we:

- Reviewed Federal regulations, Department directives, Office of Management and Budget guidance, and other policies and guidance pertaining to cybersecurity risk management;
- Reviewed prior reports issued by the Office of Inspector General and the Government Accountability Office and corrective actions taken in response to those reports;
- Evaluated security plans and supporting documents for 25 systems to determine whether potential opportunities existed for improving the Department's cybersecurity posture;
- Determined whether organizations and sites established performance metrics and goals specific to management of cybersecurity risks and oversight of contractor systems; and
- Held discussions with program officials and personnel from Department Headquarters and field sites reviewed, including representatives from the Offices of the Chief Information Officer; Chief Financial Officer; Science; Fossil Energy; Nuclear Energy;

Energy Efficiency and Renewable Energy; Environmental Management; Environment, Health, Safety, and Security; and Enterprise Assessments; as well as the National Nuclear Security Administration.

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 objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusion based on our 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 *GPRA Modernization Act of 2010* and determined that it had not established performance measures for cybersecurity risk management. 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 rely on computer-processed data to satisfy our objective.

An exit conference was held with Office of Environmental Management officials on October 20, 2015. An exit conference was held with Office of Chief Information Officer officials on November 2, 2015. Management from each of the other Department elements reviewed waived an exit conference.

PRIOR REPORTS

- Evaluation Report on *The Department of Energy's Unclassified Cybersecurity Program - 2014* (DOE/IG-0925, October 2014). While the Department of Energy (Department) and the National Nuclear Security Administration (NNSA) had taken positive actions to correct deficiencies identified in prior years, additional effort was needed to ensure that the risks to operating systems were identified and that systems and information were adequately secured. For example, we noted issues pertaining to reporting contractor systems performance metrics, patch management, system integrity, logical access controls, configuration management, and security management. The issues identified occurred, at least in part, because the Department's programs and sites had not ensured that cybersecurity policies and procedures were developed and properly implemented. The weaknesses identified in this report should be thoroughly considered as the Department transitions its cybersecurity program from the traditional compliance-based process to one that supports the National Institute of Standards and Technology's risk management framework and continuous system authorizations.

- Audit Report on *The Department of Energy's Management of Cloud Computing Activities* (DOE/IG-0918, September 2014). The Department had not always effectively or efficiently acquired, implemented, or managed its cloud computing technologies. In particular, the Department had not always established contracts with cloud computing service providers that ensured effective controls over the management of stored or transmitted information. In addition, the Department had not ensured that cloud computing services were implemented in accordance with the Federal Risk and Authorization Management Program. These issues occurred, in part, because the Department lacked a comprehensive strategy designed to ensure effective and efficient implementation of cloud computing technologies. Furthermore, programs and sites had not implemented risk management processes to ensure that critical oversight controls were in place related to access to facilities and data, establishment of service level agreements used to define acceptable levels of service, and the ability to conduct audits and investigations related to cloud computing contracts. Moreover, moving systems and data into the cloud without an effective strategy, policy, or adequate risk management practices can result in cloud computing technologies that fail to meet mission needs and key business or information technology security requirements.

- Special Report on *Office of Energy Efficiency and Renewable Energy's Integrated Resource and Information System* (DOE/IG-0905, April 2014). The Office of Energy Efficiency and Renewable Energy (EERE) had not effectively managed the development and implementation of the Integrated Resource and Information System (IRIS). In particular, EERE failed to follow the Department's structured capital planning and investment control process and had not provided effective monitoring of the project. Also, EERE had not implemented key cybersecurity controls designed to protect IRIS and the network on which it resided. EERE also had not entered into an agreement with the application's vendor prior to beginning use of the system to ensure that acceptable service levels for operations were agreed upon, a key control when implementing cloud computing technology. Without a well-defined project planning and execution process,

EERE could not ensure that significant funds spent on IRIS and other future information technology projects were used in a cost effective manner. In addition, by introducing systems that had not met the necessary cybersecurity requirements, the Department ran an increased risk that the confidentiality, integrity, and availability of systems and information could be compromised.

- Special Report on *The Department of Energy's July 2013 Cyber Security Breach* (DOE/IG-0900, December 2013). The July 2013 incident resulted in the exfiltration of a variety of personally identifiable information on over 104,000 individuals. Our review identified a number of technical and management issues that contributed to an environment in which this breach was possible. Compliance and technical problems included the frequent use of complete social security numbers as identifiers; permitting direct internet access to a highly sensitive system without adequate security controls; lack of assurance that required security planning and testing activities were conducted; and failure to assign the appropriate level of urgency to replace end-of-life systems. We also identified numerous contributing factors related to inadequate management processes. These issues created an environment in which the cybersecurity weaknesses we observed could go undetected and/or uncorrected. While we did not identify a single point of failure that led to the breach, the combination of the technical and managerial problems we observed set the stage for individuals with malicious intent to access the system with what appeared to be relative ease.

- Audit Report on *Management of Naval Reactors' Cyber Security Program* (DOE/IG-0884, April 2013). Weaknesses related to vulnerability management, access controls, incident response, and security awareness training were identified that could negatively affect the Naval Reactors Program security posture. The weaknesses identified occurred, in part, because the Naval Reactors Program had not ensured that necessary cybersecurity controls were fully implemented. Absent a fully effective cybersecurity program, information systems and data remain at 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 Los Alamos National Laboratory (LANL) had not fully implemented its risk management, system security testing, and vulnerability management practices. 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 practices that were less rigorous than those required by Federal directives. In addition, we found that LANL's Information Technology Directorate had not followed NNSA policies and guidance for assessing system risk and had not fully implemented the Laboratory'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
Washington, DC 20585

September 11, 2015

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

FROM: MICHAEL M. JOHNSON ajm for
CHIEF INFORMATION OFFICER

SUBJECT: Inspector General Audit Draft Report (IG-37) for the Department of Energy's Cybersecurity Risk Management Framework (A14TG041).

Thank you for providing a copy of the Inspector General Audit Draft Report (IG-37) for the Department of Energy's Cybersecurity Risk Management Framework (A14TG041). The information in the report will enable the Department to continue to work in the most effective way to improve the Department's security posture. We have reviewed the draft report and a summary of our comments follow. Refer to the Attachment for details on the following.

- **Response to Recommendations:**
  Refer to the Enclosure for detailed comments from the Office of the Chief Information Office (OCIO), Office of Science (SC), National Nuclear Security Agency (NNSA)/NNSA Production Office (NPO) Y-12, and the Office of Energy Efficiency and Renewable Energy (EERE), Golden Field Office (GFO).

- **Response to Technical and General Comments:**
  Refer to the Enclosure for comments from the SC, EERE/GFO and NPO-Y12.

- **Response to Memo Points:**
  No comments.

If you have any questions, please contact Paul Cunningham, Acting Chief Information Security Officer, at 202-586-9805.

Attachment

Enclosure

Response to Draft Audit Report "The Department of Energy's Cybersecurity Risk Management Framework, IG-37 (A14TG041)
September 2015 Version

Office of the Chief Information Office (OCIO) Response to Report Recommendations

RESPONSE TO RECOMMENDATIONS:

- **Recommendation 1.** *Develop, implement, and maintain Department, program, and site level cybersecurity policies and procedures that are consistent with current Federal requirements and best practices.*

  Management Response: Concur

  At the Department and program level, the DOE Order (O) 205.1B, Department of Energy Cyber Security Program, codifies a federated risk-based approach to cybersecurity planning across the Department. The Departmental program requires a Risk Management Approach (RMA) that includes analysis of threats/risks; risk-based decisions considering security, cost, and mission effectiveness; and implementation consistent with guidelines from the National Institute of Standards and Technology (NIST) cyber requirements, processes, and protections. The Federal Information Security Management Act (FISMA) FY15 Quarterly Reports results illustrate the progress DOE organizations have made in addressing risks to and vulnerabilities in information systems and data. DOE organizations maintain Plans of Actions and Milestones (POA&Ms) to track mitigations of identified vulnerabilities at the systems and program levels. POA&Ms are extensive and detailed and are utilized locally to prioritize activities to remediate issues. The Order is being updated to support the NIST's Risk Management Framework (RMF) and include federal requirements and best practices to ensure risk management processes in place.

  Estimated Completion Date:

- **Recommendation 1.** estimated completion March 31, 2016

- **Recommendation 2.** *Develop and implement effective oversight and communication of cybersecurity risk management practices by:*

  a. *Ensuring that continuous authorization processes are approved only when they can be adequately supported and sufficiently resourced;*

  b. *Ensuring that POA&M processes are complete and effectively implemented; and*

  c. *Establishing and communicating risk tolerance levels for Department elements, as appropriate, and consistently relaying all known weaknesses to risk acceptance officials.*

  Management Response: Concur 2a, 2b, 2c

Enclosure

Response to Draft Audit Report "The Department of Energy's Cybersecurity Risk Management Framework, IG-37 (A14TG041)
September 2015 Version

The Department is working to ensure organizations implement a risk-based approach to cybersecurity within their programs and systems with the following methods.

a. Recommendation 2a. Develop and implement effective continuous authorization processes that have been approved and can be properly supported and resourced.

b. Recommendation 2b. Continue to develop and continue to implement effective POA&M processes that provide greater consistency and accuracy in reported POA&M data. The Enterprise Cyber Governance (ECGS) system provides an automated enterprise governance, risk, and compliance capability for POA&M management and reporting and is automating previous manual processes.

c. Recommendation 2c. Develop an enterprise-wide approach and best practices for risk management. Incorporate continuous monitoring and vulnerability assessment and remediation in order to support informed risk management decisions.

Estimated Completion Date:

- Recommendation 2a estimated completion date is September 30, 2016
- Recommendation 2b estimated completion date is September 30, 2016
- Recommendation 2c estimated completion date is September 30, 2016

2

Enclosure

Response to Draft Audit Report "The Department of Energy's Cybersecurity Risk Management Framework, IG-37 (A14TG041)
September 2015 Version

Office of Science

RESPONSE TO RECOMMENDATIONS:

Recommendation 1: *Develop, implement, and maintain Department, program, and site level cybersecurity policies and procedures that are consistent with current Federal requirements and best practices.*

Management Response: Concur.

Action Plan: SC will develop and promulgate SC site requirements for the development, implementation and maintenance of Continuous Monitoring and Authorization for SC Information Systems. Assessment of those requirements will be included in site oversight of cyber security. SC will include assessment of these requirements in the SC Safeguards and Security Survey planning to assess whether sites are utilizing the new requirements.

Estimated Completion Date: September 30, 2016

Recommendation 2: *Develop and implement effective oversight and communication of cybersecurity risk management practices by:*

a. *Ensuring that continuous authorization processes are approved only when they can be adequately supported and sufficiently resources.*

   Management Response: Partially concur. Reasons cited in Technical Comments, number 5

   Action Plan: SC will develop and promulgate SC site requirements for the development, implementation and maintenance of Continuous Monitoring and Authorization for SC Information Systems. Assessment of those requirements will be included in site oversight of cyber security. SC will include assessment of these requirements in the SC Safeguards and Security Survey planning to assess whether sites are utilizing the new requirements.

   Estimated Completion Date: September 30, 2016

b. *Ensuring that POA&M processes are complete and effectively implemented.*

   Management Response: Concur

   Action Plan: No action necessary. SC has a robust process in place for ensuring POA&M processes are complete and effectively implemented.

   Estimated Completion Date: NA

3

Enclosure

Response to Draft Audit Report "The Department of Energy's Cybersecurity Risk Management Framework, IG-37 (A14TG041)
September 2015 Version

c. *Establishing and communicating risk tolerance levels for Department elements, as appropriate, and consistently relaying all known weaknesses to risk acceptance officials.*

Management Response: Concur

Action Plan: SC will develop guidance for determining risk tolerance levels for SC sites including communicating the current state of risk (e.g., threats and weaknesses) associated with the information system to the authorizing official.

Estimated Completion Date: September 30, 2016

Enclosure

Response to Draft Audit Report "The Department of Energy's Cybersecurity Risk Management Framework, IG-37 (A14TG041)
September 2015 Version

Office of Energy Efficiency and Renewable Energy, Golden Field Office Response to Report Recommendations

RESPONSE TO RECOMMENDATIONS:

Recommendation 1: Develop, implement, and maintain Department, program, and site level cybersecurity policies and procedures that are consistent with current Federal requirements and best practices.

Management Response: EERE Concurs.

Recommendation 2: Develop and implement effective oversight and communication of cybersecurity risk management practices by:

a. Ensuring that continuous authorization processes are approved only when they can be adequately supported and sufficiently resources.

b. Ensuring that POA&M processes are complete and effectively implemented.

c. Establishing and communicating risk tolerance levels for Department elements, as appropriate, and consistently relaying all known weaknesses to risk acceptance officials.

Management Response: Concur.

Action Plan: We concur with the report findings on the current state of the Risk Management Framework at NREL. NREL has an active Plan of Actions and Milestones (POA&M) item due in late November, 2015, for the initial submission of a Contractor Assurance System (CAS) that is fully in line with the Department of Energy Risk Management Framework. Our National Laboratory Oversight Office will thoroughly review it and work with NREL to approve a CAS that will transition the Lab to a risk-based cybersecurity program that is monitored and evaluated for effectiveness, and one that will continually mature to fully meet Federal requirements.

5

Enclosure

Response to Draft Audit Report "The Department of Energy's Cybersecurity Risk Management Framework, IG-37 (A14TG041)
September 2015 Version

NNSA Response to Report Recommendations

RESPONSE TO RECOMMENDATIONS:

Recommendation 1: *Develop, implement, and maintain Department, program, and site level cybersecurity policies and procedures that are consistent with current Federal requirements and best practices.*

Management Response: Partial concur

1) The Department of Energy (DOE) has developed and issued DOE O 205.1B and the NNSA has developed and issued NAP 14.1D, both of which provides direction to the contractor for the implementation of a comprehensive cybersecurity program. NNSA OCIO is not in full agreement with the IG where they make the statement that the findings were due to lack of departmental and/or program policy, as the examples of the findings cited there were issues with application of policies and procedures not an issue with updates or missing references to Departmental or NNSA policy. NNSA considers this action completed as there is no further action required.

   Estimated Completion Date: N/A.

Recommendation 2: *Develop and implement effective oversight and communication of cybersecurity risk management practices by:*

Management Response: Concur Rec 2a; 2b and 2c

a. *Ensuring that continuous authorization processes are approved only when they can be adequately supported and sufficiently resourced;*

   Recommendation 2a. NA-IM, through its implementation of the RSA Archer GRC technology, is committed to extending continuous monitoring of applicable security controls. That commitment supports the evolution to "continuous authorizations". However, that approval to evolve appropriate technologies only serve to support NNSA AOs in their authorization-to-operate decisions. For NNSA AOs, security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect NNSA information. Data collection, no matter how frequent, is performed at discrete intervals. Ongoing authorization guidance does not change current OMB policies or NIST guidance with regard to risk management, information security, security categorization, security control selection, implementation, assessment, continuous monitoring, or security authorization. NNSA considers this action completed as there is no further action required.

   Estimated Completion Date: N/A.

Enclosure

Response to Draft Audit Report "The Department of Energy's Cybersecurity Risk Management Framework, IG-37 (A14TG041)
September 2015 Version

b. *Ensuring that POA&M processes are complete and effectively implemented*

Recommendation 2b. NNSA OCIO is committed to the development and implementation of processes and procedures that will ensure the completion and effectiveness of the POA&M process. NNSA OCIO has matured its oversight assessment process to include assessment of POA&M processes to ensure they are complete and effectively implemented. Additionally, NA-IM-10 plans to conduct POA&M process training which includes mandatory application of RSA Archer GRC technology.

Estimated Completion Date: April 30, 2016.

c. *Establishing and communicating risk tolerance levels for Department elements, as appropriate, and consistently relaying all known weaknesses to risk acceptance officials.*

Recommendation 2c. NA-IM, through its implementation of the Enterprise Cyber Security Advisory Board (ECSAB) and RSA Archer GRC technology, is committed to the establishment and implementation of processes and procedures that will ensure that all risk elements are communicated to departmental risk official.

Estimated Completion Date: December 30, 2016.

7

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. You may also mail comments to us:

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.