U.S. Department of Energy

Office of Inspector General

Office of Audits and Inspections

AUDIT REPORT

The Energy Information Administration's Information Technology Program

DOE-OIG-16-04

November 2015

Department of Energy
Washington, DC 20585

November 17, 2015

MEMORANDUM FOR THE SECRETARY

FROM: Rickey R. Hass
Acting Inspector General

SUBJECT: INFORMATION: Audit Report: "The Energy Information Administration's Information Technology Program"

BACKGROUND

The Energy Information Administration (EIA) is a statistical and analytical agency within the Department of Energy responsible for a wide range of data collection, analysis, forecasting, and dissemination of energy information. To support its mission, EIA makes extensive use of information technology (IT) resources related to infrastructure, shared technology services, Web content, and data management. EIA's four program offices—the Offices of Resource and Technology Management, Energy Statistics, Energy Analysis, and Communication—are responsible for managing various aspects of EIA's infrastructure, financial, and mission-related activities. Using information provided by EIA during our review, we determined the four offices spent approximately $53 million on IT activities during fiscal years 2012 through 2014.

The Office of Inspector General received four allegations expressing concerns with various aspects of EIA's IT program. Specifically, the complainants alleged problems with management of IT funds, reporting inconsistencies of IT investments, and mismanagement of records. In addition, the complainants alleged that EIA's Transformation Project, a major system development effort designed to enhance efficiencies within the agency, produced no significant results or benefit and resulted in wasted funds and resources. In response, we initiated this audit to determine whether EIA implemented and managed an effective IT program.

RESULTS OF AUDIT

Our review largely substantiated the allegations related to IT and records management. Based on these findings, we determined that EIA had not implemented a fully effective IT program. In particular, we identified weaknesses related to IT project management, capital planning and investment control, cybersecurity, and records management. We found the following:

- Although the Transformation Project had been in development since April 2011 and cost EIA almost $20 million to date, the project was not implemented using sound project management practices and remained incomplete. For instance, officials had not

completed a cost/benefit or alternatives analysis prior to beginning the project and had not developed cost estimates, schedules, or performance metrics to guide implementation of the Transformation Project. In addition, even though a primary goal of the Transformation Project was to modernize EIA's environment and create process efficiencies, no legacy processes had been transitioned to the project at the time of our review.

- Although specifically required, we determined that a significant portion of EIA's IT costs had not been reported to the Office of Management and Budget (OMB). While agencies are required to submit an accounting of IT investments annually to OMB, EIA only reported IT costs of approximately $27 million for fiscal years 2012 through 2014, even though actual expenditures were about $53 million. Management officials told us that even though the Transformation Project was designed to modernize EIA's environment, program officials decided not to include costs for the project in those reported to OMB. Had the required cost reporting been done, it could have led to the identification of the effort as a major IT investment. Such an action would have required formalized project documentation and enhanced oversight.

- Numerous cybersecurity weaknesses existed. For instance, we identified systems and applications that were not always updated with the latest version or were missing security patches released more than a year prior to our testing. In addition, EIA employed software that was no longer supported by the vendor, leaving potential vulnerabilities unmitigated. We also found that officials may not have appropriately categorized the risk to systems and implemented all necessary controls. We noted that security controls related to areas such as access controls, contingency planning, and system and information integrity were not implemented in accordance with Federal requirements.

- As alleged in one of the complaints, EIA had not implemented a comprehensive and effective records management program. Specifically, each of the four EIA program offices independently managed their own records and did not adhere to Federal records management requirements and guidance. In addition, officials had not ensured that records management functions were included in the design and implementation of system development efforts, including the aforementioned Transformation Project.

The weaknesses identified occurred, in part, because EIA management had not ensured that applicable Federal and Department policies and procedures were always implemented. For instance, while Department Order 200.1A, *Information Technology Management*, required that organizations demonstrate effective control of the cost, scope, and schedule of investments and corresponding projects, we found that EIA did not always take such action. Also, EIA had not fully implemented cybersecurity controls in accordance with Federal and Department requirements. Furthermore, EIA had not implemented an effective governance structure over IT project management and cybersecurity activities. For example, EIA officials had not fully developed and implemented an enterprise architecture or strategic planning process that could have helped EIA realize its desired IT infrastructure in an organized and timely manner. In addition, confusion regarding lines of authority adversely affected EIA's cybersecurity, project

management, and records management programs. We noted that a number of weaknesses related to these areas may have been alleviated had EIA implemented a centralized approach to management.

To its credit, EIA had begun to address certain known issues with its IT program. For example, officials told us that the authority for program offices to make decisions affecting the EIA infrastructure independent of the Office of Information Technology was recently rescinded. In addition, EIA improved its cybersecurity posture by reducing the number of personnel with elevated access privileges to information systems. While these actions are commendable, without additional corrective measures, EIA may continue to encounter project management weaknesses and operate its information systems at a higher-than-necessary level of risk. As such, we have made recommendations that, if fully implemented, should improve management of EIA's IT and records management programs.

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 response and planned actions are responsive to our recommendations. Management's comments and our responses are summarized in the body of the report. Management's formal comments are included in Appendix 3.

Attachments

cc: Deputy Secretary
Administrator for the Energy Information Administration
Under Secretary for Science and Energy
Deputy Under Secretary for Management and Performance
Chief of Staff
Chief Information Officer

AUDIT REPORT: THE ENERGY INFORMATION ADMINISTRATION'S INFORMATION TECHNOLOGY PROGRAM

TABLE OF CONTENTS

Audit Report

Appendices

THE ENERGY INFORMATION ADMINISTRATION'S INFORMATION TECHNOLOGY PROGRAM

DETAILS OF FINDING

The Office of Inspector General received multiple allegations related to the Energy Information Administration (EIA) implementation and management of its information technology (IT) program. Most notably, the complainants alleged that the Transformation Project was not properly managed. It was alleged that the project, which was designed to provide process efficiencies within the agency, had not been effectively implemented, produced no significant results or benefit, and resulted in wasted funds and resources. The remaining allegations asserted that EIA mismanaged IT funds and did not report accurate and complete IT investment costs to the Department of Energy (Department) and the Office of Management and Budget (OMB), as required. It was also alleged that the management of records was ineffective and did not adhere to Federal requirements.

Our review largely substantiated the allegations and determined that EIA had not fully implemented and managed an effective IT program. Specifically, we identified weaknesses related to the Transformation Project, including the planning, implementation, and management of the project. In addition, we identified that EIA IT investment costs were not always reported to OMB as required by the Department's Capital Planning and Investment Control (CPIC) process. We also found numerous cybersecurity weaknesses related to the management of EIA's information systems. Furthermore, EIA lacked a comprehensive and effective records management program.

Transformation Project Management

Although the Transformation Project—an ongoing initiative intended to centralize and reduce the number of software applications used for energy survey data collection and management—had been in development since April 2011 and cost almost $20 million, it was not implemented using an effective project management process. For instance, although required by the Department's CPIC process, EIA had not completed a cost-benefit or alternatives analysis prior to initiating the Transformation Project. In addition, officials had not established schedules and milestones to guide development and implementation, and there were no metrics to measure the project's performance. Essential planning activities such as these could have helped ensure that the project met business and mission needs and aligned with organizational strategic goals in a timely manner.

Furthermore, EIA officials had not developed cost estimates or tracked costs since the initiation of the Transformation Project. Specifically, officials were unable to provide the total costs of the Transformation Project and noted that costs had not been properly identified and tracked from the beginning of the project. In response to requests during our review, officials reviewed project documentation such as invoices and estimated that project costs were almost $20 million as of July 2015. However, the officials noted that the costs were not tracked as a matter of course and commented that the estimate excluded certain labor costs they could not identify.

Despite more than 4 years of effort and significant cost, no legacy surveys had been fully transitioned to the new Transformation Project platform. Surveys are used by EIA to collect

usage data on energy resources such as coal, oil, and natural gas and are then analyzed, processed, and disseminated to customers. Legacy surveys have been developed over time and operate on many different technology platforms that are outdated, not standardized, and inefficient. While four surveys used portions of the new Transformation Project platform, we found that the only survey fully using the platform was a brand new survey that had not been operating on the legacy infrastructure. As such, the ongoing inefficiencies that existed by using the legacy infrastructure were not remediated. We also determined that while a plan existed for transitioning some of the remaining 65 survey applications to the Transformation Project, it did not include all surveys. For instance, surveys that collected important information related to crude oil, regulated and unregulated electric power plants, and proposed electricity generators were not part of the transition plan. As such, managing surveys in the new platform and the legacy environment may be difficult and costly.

We also identified issues related to contracting for Transformation Project services. In particular, officials entered into a contract for cloud computing services to support the initiative that did not meet Federal requirements. Rather than using EIA procurement officials, project officials worked with Department procurement personnel to complete a sole source acquisition of cloud infrastructure services using the Department's IT support contractor. As a result, EIA acquired cloud services that were not certified through the Federal Risk and Authorization Management Program (FedRAMP) process and were not appropriately competed.[1] The Office of Information Technology, EIA's infrastructure support and operations group, was only made aware of the use of the non-FedRAMP-certified provider of cloud services while conducting network scanning after it had been implemented.

To their credit, EIA officials took action to disable the connection and worked through the proper procurement process to acquire new, properly certified cloud services. However, we determined that EIA spent more than $157,000 on the cloud computing services that were only used for 3 months and ultimately disconnected. Absent adequate contracting practices, EIA may have paid more than necessary for cloud computing services and used services that did not meet all necessary cybersecurity requirements. Based on the results of our review, we substantiated allegations that EIA's ineffective management of the Transformation Project included inadequate project planning, uncoordinated system acquisitions and development, and the inaccurate tracking and reporting of project costs. We also substantiated the allegation that the project had produced very limited results and had made inefficient use of funds and other resources.

Information Technology Capital Planning

Contrary to Federal requirements, EIA IT investment costs were not always reported to OMB as part of the CPIC process. Specifically, EIA only reported approximately $27 million in IT investments during fiscal years (FYs) 2012 through 2014 even though we determined the agency spent about $53 million during that period. For instance, EIA reported total agency IT costs of just over $6 million annually for FY 2012 and 2013 when actual IT costs exceeded $14 million. The reported investments included IT costs incurred by the Office of Information Technology

[1] The Federal Risk and Authorization Management Program is a Government-wide program that provides a standardized and centralized approach to assessing cybersecurity controls and authorizing cloud computing services for operation.

but did not include any of the other three EIA program offices. Similarly, EIA only reported FY 2014 IT costs of $14 million to OMB even though it spent more than $24 million. Based on our review, we identified that costs related to cloud computing resources and information system acquisition and development were not reported as required.

We also noted that a significant portion of the costs that were not reported to OMB related to the Transformation Project. Specifically, the initiative was not reported as a major IT investment as part of the OMB Exhibit 300 process even though it met certain qualifying criteria. The Department's *Guide to IT Capital Planning and Investment Control* outlines a major IT investment as an investment that has significant program or policy implications, high executive visibility and/or high development, operating or maintenance costs, and should be supported by a capital asset plan that includes information for sound planning, management, and monitoring of the project. Based on the results of our review, we substantiated allegations that EIA did not appropriately manage its CPIC process and did not report all investments to OMB as required.

Cybersecurity

We identified various cybersecurity weaknesses related to EIA's information systems. In particular, our testing found numerous high and medium risk vulnerabilities on the network, multiple servers, and multiple workstations. In particular, we identified the following:

- Numerous systems were not updated with the most recent security patches and/or used outdated software no longer supported by the vendor. For instance, we identified at least 80 workstations that contained high risk vulnerabilities related to software such as Web browsers and office automation products. In some instances, we noted vulnerabilities on servers that were almost 10 years old. For example, we identified a 2005 server configuration vulnerability on more than 75 servers on the EIA network. In addition, our testing identified a system that was using server management software that was no longer supported by the vendor.

- In one instance, a server system was running a user service operating with default credentials for an administrator account. This type of vulnerability could have permitted unauthorized access and control of the affected system. In addition, a system was running software susceptible to common attacks, which could have permitted an attacker to run malicious code and/or crash the system.

- Application functionality allowed for the potential bypass of access controls due to the use of default credentials and lack of input data validation. Exploitation of this type of vulnerability could have allowed an attacker to obtain user credentials, steal information, or potentially execute malicious code on the system.

Officials commented that compensating controls had been implemented in some instances and/or security patches were in the process of being applied. In addition, while officials asserted that some of the vulnerabilities were considered low risk, we noted that EIA officials had not

appropriately considered the risks associated with the patches during the risk assessment process. Without remediation of the identified vulnerabilities, an attacker could gain unauthorized access to EIA systems and information.

In light of the importance of EIA's information systems to its mission and the needs of external stakeholders, we determined that officials may not have appropriately categorized the risk to systems and implemented all necessary related controls. Specifically, even though EIA's general support system included all infrastructure and systems used to support the agency's mission, it was only categorized as a moderate risk system. As a result, many key controls related to areas such as access control, configuration management, and contingency planning were not implemented; implementation could have enhanced the confidentiality, integrity, and availability of information in the system. Furthermore, despite its importance, officials had not identified the general support system as mission critical. EIA cybersecurity officials stated the system was not mission critical because backups were created nightly. However, we found that not all EIA data was backed up in a timely manner, including data supporting one of the weekly reports EIA identified as critical due to the impact of its release on the energy markets. In addition, although EIA had developed a Disaster Recovery Plan for addressing the loss of the system, it had not been fully tested.

We also identified weaknesses related to implementation and testing of the general support system security controls. In particular, although there were significant changes to the system environment, and the security plan was updated in June and November of 2014, officials had not used the most recent version of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, issued in April 2013, as required. As a result, 10 controls and 37 control enhancements may not have been implemented related to areas such as access controls and configuration management. Even when controls were implemented using the now outdated guidance, we found that 50 of 263 (19 percent) required controls related to various security areas were not implemented properly. For example, although the system security plan indicated that external connections were prohibited, EIA used external cloud computing services as part of the Transformation Project. Further, while the security plan noted that access controls were in place and effective at the time of our review, we identified multiple access control weaknesses. For instance, we identified an individual who still had access to a system even though access was no longer required. In addition, users for one major system were not required to review and sign a user policy, even though all users had elevated privileges that allowed them to make changes to the source code of models in the system.

Records Management

EIA had not implemented a comprehensive and effective records management program. Specifically, each of the four EIA program offices independently managed their own records and did not adhere to Federal or Department records management requirements and guidance. For example, contrary to Department guidance, the Office of Energy Analysis, which operates and maintains the National Energy Modeling System (NEMS) used to project energy-economy activities, did not incorporate records management requirements into the development, operation, or maintenance of the system. NEMS officials commented that they were not aware of the

requirements for maintaining electronic and physical records. In fact, officials stated that they maintained boxes of physical records in their office but had not conducted or maintained a records management inventory or related disposition schedule. Similarly, records management planning was not included in the design and implementation of the Transformation Project.

The issues identified during our review were similar to those identified in the National Archives and Records Administration (NARA) *2013 Records Management Self-Assessment Report*. During the assessment, EIA received a score of only 27 out of 100, elevating the risk level for the agency from moderate to high risk. The assessment noted that decentralized program management and exclusion of records management functionality from the system design and implementation process, among other issues, contributed to the change in risk level. As a result, EIA was the only Department element that received a high risk rating. Based upon our review, we substantiated allegations that EIA did not properly implement an effective records management program.

Requirements, Governance, and Management Authority

The weaknesses identified occurred, in part, because EIA officials had not ensured that applicable Federal and Department requirements related to project management, cybersecurity, and records management were always implemented. In addition, EIA had not implemented an effective governance structure over IT project management and cybersecurity activities. Furthermore, a number of the issues identified occurred due to the lack of appropriate management authority for EIA's Office of the Chief Information Officer.

Policies and Procedures

Officials had not fully implemented Department IT management requirements for project management. Although Department directives such as Department Order 200.1A, *Information Technology Management*, required that organizations ensure an effective CPIC process by demonstrating appropriate control of cost, scope, and schedule of investments and projects, we found that EIA officials had not developed a project plan, cost-benefit analysis, or alternatives analysis when the Transformation Project was initiated. In addition, milestones and deadlines were not established to evaluate ongoing project performance. EIA officials told us they did not consider the Transformation Project to be an IT project and asserted that it was not required to adhere to Department Order 415.1, *Information Technology Project Management*, because it was expected to cost less than $25 million. However, we determined that the Transformation Project should have been identified as an IT project because it was expected to fundamentally alter the methods by which data was collected and analyzed, change internal business processes, and result in new IT resources to replace aging legacy systems. Without adequate project planning, EIA could not ensure that the Transformation Project met all applicable requirements and was completed in the most effective, economical, and timely manner.

EIA also had not implemented cybersecurity controls in accordance with Federal and Department requirements. We found that various weaknesses occurred because EIA failed to fully implement controls related to patch management, configuration management, or access controls. For example, although the system security plan noted that external connections were

prohibited, we found that EIA was using cloud services through an external provider. However, the related security control on the use of external information systems was not reviewed and updated in accordance with Federal requirements even though both the IT environment and NIST guidance had changed. In addition, EIA began operating a new data center in April 2013, using virtualization; however, the system controls were not reevaluated for this significant change as required by NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*. Therefore, the authority to operate the system was based on inaccurate and outdated system security information. Furthermore, steps related to an effective Risk Management Framework identified in NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, were not fully implemented for the general support system, including implementation and monitoring of security controls and residual risk management. As a result, the system was operating at an unnecessarily elevated risk.

Officials also had not implemented records management requirements in accordance with Department and NARA guidance. For example, although required by Department Order 243.1B, *Records Management Program*, EIA did not use a centralized records management structure to ensure effectiveness and consistency within the organization. In addition, while EIA had an Agency Records Officer in place, he lacked the authority to ensure program office compliance with records management requirements such as maintaining records inventories and the identification, storage, and disposition of agency records. EIA also had not incorporated records management functionality into the agency's system development and design process, as required. For example, officials did not include records management planning into the design and implementation of the Transformation Project. Also, contrary to NARA Bulletins 2013-3 and 2014-6, EIA did not issue guidance to staff concerning the identification, management, retention, and disposition of Federal records, including electronic records and emails. Similarly, training related to managing employee records was not provided as required.

Governance and Planning

Many of the identified weaknesses within EIA were also caused by the lack of an effective governance structure. Although OMB identified governance as a key element in ensuring an effective IT program in *The Common Approach to Federal Enterprise Architecture*, EIA had not established a centralized IT management structure to provide enterprise-wide oversight to its IT program. For example, the Office of Energy Statistics, the office responsible for managing the Transformation Project, had authority to make decisions that affected the EIA infrastructure without working through the subject matter experts and infrastructure owners in the Office of Information Technology. In addition, EIA had not implemented an effective IT governance board that included participants from all program offices. While an IT review committee was established and included members from each of the four program offices, some officials noted that the committee resided at too low of an organizational level and lacked the authority to be effective. In addition, senior EIA officials identified an ineffective governance process as a key reason for some of the issues identified with the IT program during our audit. For example, officials commented that the lack of an effective governance structure led to the operation of a cloud computing system without the full participation and knowledge of key IT program officials, resulting in the premature shutdown of the system.

We also determined that EIA had not implemented effective strategic planning processes to help manage its IT program. For example, EIA officials had not established an enterprise architecture or updated the IT Strategic Plan, both critical components of effective strategic planning. An enterprise architecture plan describes the current state and future vision of an agency's IT design and operations, as well as the plan for transitioning from current to future system architectures. Similarly, an effective IT strategic plan could have supported EIA by illustrating the strategic use of information resources, as well as ensuring information resources are integrated throughout the organization. In addition, required planning procedures intended to align IT resources to the agency's Strategic Plan were missing, outdated, or ineffective. For example, EIA officials had not documented a CPIC process that linked mission needs with IT resources. Absent these key strategic planning resources, EIA did not manage its IT resources in the most efficient and effective manner.

Management Authority

We noted that lines of authority adversely affected EIA's cybersecurity, project management, and records management programs. In particular, contrary to Federal regulations, the EIA Chief Information Officer (CIO) did not have the appropriate level of insight and authority to make a number of IT decisions throughout the organization or implement necessary corrective actions. For example, even though EIA's Office of Information Technology conducted various testing to identify vulnerabilities on information systems across EIA's programs, the office did not have the authority to remediate the vulnerabilities. Cybersecurity officials told us that when vulnerabilities were identified, they were immediately passed along to the appropriate offices for remediation. However, our testing found that 2 of the 11 high risk vulnerabilities identified during our scanning, affecting both servers and workstations, were previously identified by EIA's internal scanning process and were never remediated. We also found that the CIO was not included in the design and implementation of the Transformation Project developed within the Office of Energy Statistics. As such, officials from the Office of Energy Statistics independently decided to use a cloud computing system that did not meet Federal requirements and were ultimately required to stop using the system. Federal regulations require that the CIO is responsible for developing and maintaining an agency's information security program and ensuring IT resources are acquired and managed in an effective manner. Recent legislation also reinforced the CIO's role in planning, budgeting, and acquiring IT resources within Federal agencies. Had EIA empowered its CIO as envisioned by Federal requirements, many of the weaknesses identified during our review may not have occurred.

Similarly, the records management issues identified were primarily due to the lack of a centralized authority for ensuring policies and procedures were developed, implemented, and enforced. Contrary to OMB requirements, EIA had not established a records management Senior Agency Official to be directly responsible for ensuring the organization efficiently and appropriately complied with all applicable records management requirements. Although EIA had an Agency Records Officer, he had limited authority and insight into the program offices and was not included in any strategic discussion or planning concerning records management. For example, during the development of the Transformation Project, neither the Agency Records

Officer nor any other records management subject matter expert was involved in ensuring that records management requirements were incorporated into the design and development of the new initiative.

Impact and Path Forward

Failure to make significant improvements to the IT program will result in continued negative impact to the operational efficiency of EIA. For instance, the mission of the agency may be affected as aging systems are updated or replaced without the necessary oversight and planning. Specifically, the EIA IT resource infrastructure may remain fragmented with many outdated and underperforming systems. In addition, the lack of enterprise-wide governance and oversight will perpetuate the ongoing inefficient operation of resources that are not adequately maintained and secured. Agency projects may also continue to exceed anticipated goals and milestones due to ineffective project management processes, including the lack of appropriate planning and coordination. Furthermore, the lack of accurately reported IT investment and cost information may negatively affect future EIA strategic IT planning. Our review concluded that the agency's records may also remain vulnerable due to the absence of central oversight, lack of a comprehensive inventory of records, and inconsistent management by the program offices.

RECOMMENDATIONS

To help improve EIA's IT program and ensure that it is managed effectively, we recommend the Administrator for the Energy Information Administration:

1. Ensure that applicable Federal and Department requirements pertaining to project management, cybersecurity, and records management are fully implemented, as appropriate;

2. Develop and implement an IT governance process that incorporates essential elements such as implementation of effective strategic planning, use of an enterprise architecture, and appropriate involvement of all relevant stakeholders;

3. Evaluate the position and authority of the Chief Information Officer and records management officials within the organization and make changes, as appropriate; and

4. Correct, through the implementation of appropriate controls, the specific cybersecurity weaknesses identified during our review.

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. In particular, management agreed that the clarification of the role and authority of EIA's CIO, as well as the improved employment of Federal standards for IT governance, are actions that will enable the EIA to improve the efficiency and effectiveness of the IT program. In addition, management indicated that current and ongoing efforts should address identified cybersecurity weaknesses while improving vulnerability identification capabilities. Furthermore, management noted that several initiatives intended to ensure IT programs were implemented in accordance with applicable Federal and Department requirements were underway. For example, EIA plans to establish a centralized Project Management Office to provide integrated support to all EIA programs. EIA management was also in the process of reevaluating the requirements and authority of the Agency Records Officer to ensure that individual is able to develop, implement, and direct a centralized records management program consistent with NARA guidelines.

AUDITOR COMMENTS

Management comments and the 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 Energy Information Administration (EIA) implemented and managed an effective information technology (IT) program.

Scope

The audit was performed between August 2014 and November 2015 at EIA Headquarters in Washington, DC. The audit included internal and external vulnerability scanning conducted by KPMG LLP on behalf of the Office of Inspector General. We conducted external testing of networks and systems as an outsider without any elevated privileges. We conducted internal scanning as an authenticated user (a user with a valid username and password) and reported on vulnerabilities that could be exploited by both an insider and a remote attacker. Our work did not include a determination of whether vulnerabilities found were actually exploited and used to circumvent existing controls. The audit was conducted under Office of Inspector General project number A14TG053.

Methodology

To accomplish our objective, we:

- Interviewed Federal and contractor personnel to the extent necessary to satisfy the audit objective;
- Reviewed applicable standards and guidance issued by the Department of Energy and EIA;
- Reviewed prior reports issued by the Office of Inspector General;
- Evaluated documentation pertaining to EIA's IT infrastructure, project management, systems development, enterprise architecture, capital planning process, and records management within EIA; and
- Conducted tests of cybersecurity controls for select information systems.

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 Department's implementation of the *GPRA Modernization Act of 2010* and determined that it had established performance measures for managing contracts and contractor performance. Because our review was limited, it would not have necessarily disclosed all internal control deficiencies that may have existed at the time of our audit. We did

not solely rely on computer-processed data to satisfy our objective. Computer-assisted audit tools were used to perform probes and scans of various networks and drives. We validated the results of the scans by confirming the weaknesses disclosed with responsible on-site personnel and performed other procedures to satisfy ourselves as to the reliability and competence of the data produced by the tests. In addition, we confirmed the validity of other data, when appropriate, by reviewing supporting source documents.

An exit conference was held with management on November 6, 2015.

PRIOR REPORTS

- Evaluation Report on *The Department of Energy's Unclassified Cybersecurity Program – 2014* (DOE/IG-0925, October 2014). The evaluation found that the Department of Energy (Department), including the National Nuclear Security Administration, had taken positive actions to improve the security and awareness of the unclassified cybersecurity program. However, not all deficiencies were addressed, and an additional effort was needed to ensure that the risks of operating systems were identified and that the systems and information were adequately secured. These ongoing deficiencies included the lack of reported performance metric data for contractor systems, patch management, system integrity of Web applications, access control, configuration management, and overall security management. These issues occurred, at least in part, because the Department's programs and sites 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.

- Audit Report on *The Department of Energy's Management of Cloud Computing Activities* (DOE/IG-0918, September 2014). The audit identified that the Department had not always effectively or efficiently acquired, implemented, or managed its cloud computing technologies. For example, Department programs and sites independently acquired and managed cloud computing services valued at more than $30 million. Despite the significant investment and number of cloud services in use, the Department had not developed and maintained a complete inventory of cloud services to assist in managing its efforts. Additionally, the Department had not always established contracts with cloud computing service providers that ensured effective controls over the management of information. Further, 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. In addition, officials had not provided adequate oversight to ensure that programs and sites had taken appropriate action to acquire and implement cloud computing initiatives. Lastly, programs and sites had not implemented risk management processes to ensure that critical oversight controls were in place.

- Audit Report on *The Department's Information Technology Capital Planning and Investment Control Activities* (DOE/IG-0841, September 2010). The Department had not effectively implemented a Capital Planning and Investment Control (CPIC) process for controlling and managing information technology (IT) spending. Specifically, management tools required by the Office of Management and Budget, such as IT investment portfolios and capital asset plans, had not been properly implemented. In particular, program and site officials had either not identified or had misclassified investments valued at more than $371 million in their IT investment portfolios. Additionally, major IT investments used to help accomplish the missions of the Department were not always supported by required capital asset plans. Such plans are necessary to ensure that IT initiatives are implemented in a timely and cost-effective

manner. The issues were due, in part, to problems with the Department's policy and guidance. In addition, insufficient performance monitoring and review by program office officials contributed to an ineffective CPIC process. We did find that the Department had taken certain actions to enhance its CPIC processes. However, despite these positive actions, additional effort was necessary to improve the Department's implementation of its CPIC process.

- Audit Report on *The Follow-up Audit on Retention and Management of the Department of Energy's Electronic Records* (DOE/IG-0838, September 2010). The audit found that weaknesses continued with the Department's ability to retain and manage electronic records. Specifically, the report noted that the Department programs and field sites had not ensured that electronic records, including electronic mail, were identified, stored, and disposed of properly. For example, electronic records management applications were not fully implemented or were not coordinated. The report identified that the issues occurred partially due to the ineffective implementation of electronic records management practices by Department officials. Specifically, officials had not ensured that Federal requirements were fully addressed in Department policies and guidance. Additionally, it was determined that records management was considered a low priority by management, and employees did not receive the appropriate training to identify, preserve, and dispose of electronic records. The report noted that without improvements, the Department may be unable to properly identify, store, and dispose of electronic records in an effective manner.

MANAGEMENT COMMENTS

Department of Energy
Washington, DC 20585

October 21, 2015

MEMORANDUM FOR THE INSPECTOR GENERAL, DEPARTMENT OF ENERGY

FROM: Adam Sieminski
Administrator, U.S. Energy Information Administration

SUBJECT: MANAGEMENT RESPONSE: Audit Report: "The Energy Information Administration's Information Technology Program"

The Energy Information Administration (EIA) recognizes the role of the Office of Inspector General (OIG) in promoting positive change through strengthening the integrity, economy, and efficiency of the Department's programs and operations. We concur with all of the recommendations offered in the audit report, which are both constructive and fully aligned with EIA's mission success. In particular, we agree that clarifying the role and authority of EIA's Chief Information Officer (CIO) and better employing Federal standards for Information Technology (IT) governance will enable EIA to improve the efficiency and effectiveness of our IT program.

I have directed EIA's Assistant Administrator for Resource and Technology Management to implement and monitor our action plan in response to the audit report. Further, we believe that EIA is poised to make substantial progress in migrating our energy survey program from outdated legacy systems to new systems using commercial off-the-shelf (COTS) systems, referred to in the report as EIA's Transformation Project. We will achieve this by capitalizing on recent successes with key data collection activities, including the EIA-914 (Monthly Crude Oil, Lease Condensate, and Natural Gas Production Report), the EIA-930 (Hourly and Daily Balancing Authority Operations Report), the EIA-111 (Quarterly Electricity Imports and Exports Report), the EIA-8A (Annual Survey of Coal Stocks and Coal Exports), and the EIA-22M (Monthly Biodiesel Production Survey). In order to maintain continuity in our energy survey program, some of the existing surveys are now being conducted using a hybrid of new and legacy systems during the ongoing transition.

Details of EIA's action plan in response to the audit report, including specific activities already underway, are provided below.

OIG Recommendation 1: *Ensure that applicable Federal and Department requirements pertaining to project management, cybersecurity, and records management are fully implemented, as appropriate.*

EIA Management Response: Concur.
EIA has undertaken several recent initiatives to ensure compliance with applicable Federal and Department requirements in these areas. For example, we are establishing a centralized Project Management Office to provide integrated planning, procurement, and management support to all of our programs, including IT, so that we will be positioned to demonstrate effective control of the cost, scope, and schedule of investments and corresponding projects, as required by Department Order 200.1A, *Information Technology Management*. We also recently hired a new CIO with an extensive Federal cybersecurity background, and this individual has been working collaboratively with the Department CIO to strengthen EIA's approach to IT-related risk assessment and threat mitigation. In addition, EIA's cybersecurity team is updating the agency's security plan to ensure full compliance with National Institute of Standards and Technology Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. Further, we are currently re-evaluating the requirements of EIA's recently-vacated Agency Records Officer (ARO) position so that our subsequent recruitment is targeted on a senior-level ARO with the appropriate background and experience to develop, implement, and direct a centralized records management program in compliance with National Archives and Records Administration (NARA) guidelines.
Estimated Completion Date: September 30, 2016

OIG Recommendation 2: *Develop and implement an IT governance process that incorporates essential elements such as implementation of effective strategic planning, use of an enterprise architecture, and appropriate involvement of all relevant stakeholders.*

EIA Management Response: Concur.
EIA acknowledges the importance of sound IT governance processes as foundational to an effective and compliant information management program. We have therefore initiated an overall review and assessment of our IT governance policies and procedures to identify areas in need of improvement. EIA will draw on appropriate external expertise for this assessment, which will be followed by the implementation of established best practices. In particular, EIA will review its strategic planning processes to identify any gaps or shortfalls and prepare and implement remediation plans, including formal development of an enterprise architecture plan to enable a more structured, informed planning process going forward. Similarly, EIA is reviewing the mechanisms used to engage and coordinate with internal and external stakeholders so that their interests are addressed within a formal process.
Estimated Completion Date: September 30, 2016

OIG Recommendation 3: *Evaluate the position and authority of the Chief Information Officer and records management officials within the organization and make changes, as appropriate.*

EIA Management Response: Concur.
EIA has already taken steps to address this recommendation, in particular through the hiring of a new CIO with the requisite experience to effectively coordinate and lead all aspects of our IT program. This individual has been designated as the central authority for ensuring compliance with Federal and Department requirements for IT development, operations, and security; consequently, all IT-related activities at the program office level are now directed through the CIO's office. EIA also continues to implement the provisions of the Federal Information Technology Acquisition Reform Act (FITARA), including sections addressing a common baseline of CIO roles and responsibilities and organizational self-assessments. EIA is confident that compliance with the spirit of FITARA will lead to improvements in organizational effectiveness and enhanced cybersecurity. In addition, the Senior Agency Records Officer position noted in our response to Recommendation 1 will be vested with authority under the CIO to work with program office staff to bring EIA's records management practices into compliance with applicable Federal and Department guidelines and regulations.
Estimated Completion Date: January 31, 2016

OIG Recommendation 4: *Correct, through the implementation of appropriate controls, the specific cybersecurity weaknesses identified during our review.*

EIA Management Response: Concur.
EIA has successfully remediated all but three of the 29 cybersecurity weaknesses identified by OIG. A pending vendor firmware upgrade and software product replacement will address two of the outstanding vulnerabilities by November 30, 2016; efforts are underway to eliminate the final identified weakness. We continue to monitor servers and workstations as part of a larger effort to reduce the number of users with privileged access and to increase the overall percentage of users meeting credential standards. Currently, greater than 90% of all users meet Personal Identity Verification enforcement standards, including 100% of privileged users; these compliance levels significantly exceed DOE implementation targets. EIA is also improving vulnerability identification capabilities by utilizing advanced scanning tools and creating an interactive real-time system to track and manage vulnerabilities, and we have joined the Department of Homeland Security and the DOE CIO in the implementation of the Continuous Diagnostic and Mitigation Program as part of a larger effort to monitor, identify, and address vulnerabilities.
Estimated Completion Date: Ongoing and continuous vigilance and diligence will be required.

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.