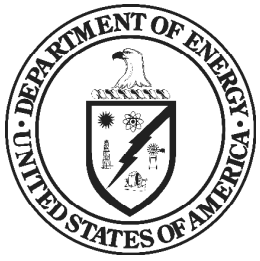

U.S. Department of Energy
Office of Inspector General
Office of Audits and Inspections

Special Report

Office of Energy Efficiency and Renewable Energy's Integrated Resource and Information System

DOE/IG-0905 April 2014

Department of Energy
Washington, DC 20585

April 3, 2014

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Special Report on the "Office of Energy Efficiency and Renewable Energy's Integrated Resource and Information System"

BACKGROUND

The Department of Energy's Office of Energy Efficiency and Renewable Energy's (EERE) mission is to accelerate development and facilitate deployment of energy technologies and market-based solutions that strengthen the Nation's energy security, environmental quality and economic vitality. To help streamline its business processes and enhance communications among employees, EERE initiated the development of the Integrated Resource and Information System (IRIS) project in October 2012. EERE officials determined that a single information technology (IT) solution was needed to replace approximately 119 existing systems and planned to use a cloud computing platform – a type of computing technology in which most or all data could be stored at the vendor's location – to support the effort. At the time of our review, EERE had spent over $7 million on the project and planned to budget an additional $3.6 million for IRIS through December 2014.

The Office of Inspector General received two complaints regarding the EERE IRIS development effort. Both complaints alleged improprieties with contract and project management. Among other things, it was alleged that officials managing the IRIS project ignored the Department's structured capital planning and investment control process for IT investments and failed to follow procurement and contracting guidelines and requirements. In addition, it was alleged that the project lacked effective oversight controls to enable Federal managers to monitor progress against baseline costs, schedules, performance and expected benefits, which resulted in significant cost overruns and implementation delays without producing any results. In response, we initiated a review to determine whether the IRIS system development effort was effectively managed.

RESULTS OF AUDIT

Our review largely substantiated the allegations related to contract and project management. We discovered that EERE had not effectively managed the development and implementation of 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.

Project Planning and Execution

We identified significant weaknesses related to IRIS project planning and execution, including a lack of project plans, schedules and budgets; ineffective identification of user requirements; and inadequate monitoring and controlling of changes to the system. We found that:

- Contrary to Federal and Department project management guidance, EERE spent at least $7 million to date on IRIS development without the benefit of formalized project plans, schedules or budgets. Such project management tools are important to establish a baseline and assess the status of major milestones, activities and deliverables to help ensure the development effort meets mission and business objectives in a timely and cost effective manner. Even though recommended by EERE staff, program officials did not develop a capital asset plan that could have provided budgetary and management information necessary for sound planning, management and monitoring of the project. Notably, EERE categorized funds being used for IRIS development as costs for other unrelated systems, thereby distorting the true cost of the project. The Office of Management and Budget personnel and the Department's Chief Information Officer were also not fully cognizant of EERE development activities and as such were unable to evaluate the effectiveness of those efforts and take corrective actions, as needed. Subsequent to our field work, EERE incorporated IRIS development baselines, cost estimates and completion dates into its Information Technology Service Office plan, which was approved in November 2013.

- Inadequate planning and identification of user requirements resulted in significant changes to the scope of the project and the acquisition of more software licenses than necessary. EERE intended to implement a commercial-off-the-shelf (COTS) product with total estimated integration costs of approximately $2.75 million. However, EERE spent $3.6 million on IRIS modifications, including more than $1.6 million to customize three IRIS modules by as much as an estimated 90 percent without a full understanding of user needs, cost and program impacts. EERE also purchased 1,000 software licenses at a cost of $1 million, of which less than 20 percent were used resulting in nearly $675,000 in unnecessary expenditures. This purchase occurred despite warnings from EERE staff regarding the risk of acquiring more licenses than necessary. In response to our review, EERE significantly reduced the number of software licenses.

- Various scope and schedule changes were made during IRIS execution without the benefit of a formal change control process. We identified various ad-hoc changes to the IRIS development effort that were made without formal approval or justification. In one instance, senior EERE officials decided to reduce the number of modules to be implemented while at the same time extending the schedule, without fully considering the impacts on the project cost/schedule.

Cyber Security

In addition, EERE had not implemented key cyber security controls designed to protect IRIS and the network on which it resided. For instance, EERE placed a module of the IRIS system into

operation prior to receiving formal authority to operate and approval of corresponding cyber security documentation. Although authority to operate the system was subsequently approved, we noted that important account management, audit log and configuration management controls still needed to be addressed. Our review also disclosed that EERE 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 both operations and security were agreed upon, a key control when implementing cloud computing technology.

Acquisition Issues

We identified troubling irregularities in aspects of the process used to select and manage the contracts for the IRIS project. For example, the method used to select the IRIS software vendor was suspect, raising questions of whether the selection was carried out in an appropriate manner. We were told by management that the selection of the COTS product occurred after an evaluation of various solutions. However, several officials we spoke with stated that they believed the decision to use the selected software vendor was made prior to the preliminary analysis being conducted. In addition, we determined that rather than using a competitive selection process for services associated with IRIS development, EERE utilized an existing IT support services contract for which the scope of work was initially limited to EERE's Golden Field Office. However, development of IRIS was conducted at Headquarters and, as such, extending the contract may not have resulted in the best value for the Government. Furthermore, contrary to Department guidance, a senior EERE official inappropriately directed contractor personnel to retain specific individuals to support the project.

Contributing Factors

It became apparent during our review that staff informed EERE management officials that IRIS was not being conducted in accordance with various project management requirements. Yet, the officials decided not to take remedial action. We recognized that the issues identified during the audit were exacerbated by the accelerated planning, development and deployment approach utilized by EERE. By accelerating the IRIS project, EERE failed to place adequate attention on implementing project management and cyber security requirements, guidance and best practices that could have helped ensure successful system implementation. For instance, program officials could have focused attention on ensuring that they followed the Department's Capital Planning and Investment Control processes, as well as both Federal and Department cyber security requirements.

Furthermore, we identified problems related to performance monitoring over the project. Specifically, the lack of a defined governance structure to monitor performance and repeated turnover of responsible project management personnel impeded the successful development and implementation of IRIS. Also, many of the practices and requirements likely could have been addressed early in the project had EERE management held open communication with the Department's Information Technology Council. However, we established that the development of IRIS was never formally communicated to the Council.

EERE Work Environment

In addition to issues previously identified, our review disclosed that problems with the work environment and poor morale within EERE clearly had an impact on program operations, including IRIS development efforts. Staff associated with the IRIS project told us they were discouraged from providing constructive feedback to management. Furthermore, many individuals we spoke with indicated they were pressured not to cooperate with the Office of Inspector General and/or expressed fear of retaliation by senior management if they openly discussed their concerns about the project. Despite these actions and what appeared to be an unhealthy environment, the vast majority of EERE staff members we interviewed and/or sought data from ultimately cooperated, and we did not observe any overt actions to frustrate our review. That said, given the environment, we cannot be fully confident that we had access to all information relevant to the IRIS project.

Impacts and Path Forward

Although EERE anticipated realizing cost savings of $1 million by implementing all 12 IRIS modules by the first quarter of Fiscal Year 2014, and retiring 119 existing systems, we found that it had only implemented 3 of 12 modules and had not retired any of the existing systems. Without a well-defined project planning and execution process that includes baselines and deliverables, EERE cannot ensure that significant funds spent on IRIS and other future IT projects are used in a cost effective manner. In addition, by introducing systems that have not met the necessary cyber security requirements, the Department runs an increased risk that the confidentiality, integrity and availability of systems and information could be compromised. Furthermore, absent contractual agreements between the Department and cloud service providers, the Department lacks assurance that acceptable performance levels and security will be maintained. Finally, staff should be encouraged and feel free to provide constructive feedback to management, without fear of reprisal. In preliminary comments on our report, EERE officials noted that fraud awareness briefings had been provided to more than 800 individuals since the start of our review. While these briefings are certainly beneficial, it is unclear to us that they alone will address work environment and/or morale issues within EERE.

The issues identified are similar to those reported during our review of *Management Controls over the Development and Implementation of the Office of Energy Efficiency and Renewable Energy's Performance and Accountability for Grants in Energy System* (OAS-RA-10-14, July 2010). Although management concurred with our prior report's recommendation to ensure that effective project management practices are implemented as part of system development and implementation efforts, the weaknesses discussed in our current report indicate that significant additional work is needed. To address these issues, we made several recommendations that, if fully implemented, should improve EERE's ability to manage future IT system development projects, improve the security posture of IRIS and ensure that appropriate contract management practices are conducted. We also made recommendations designed to facilitate a positive work environment for EERE personnel. Finally, we believe that the Department should determine whether any action should be taken against individuals responsible for the personnel and contract management issues noted in our report. The report included recommendations to this effect.

MANAGEMENT REACTION

Management concurred with the report's recommendations and indicated that it had initiated corrective actions to address our recommendations. Management's comments and our response are summarized and more fully discussed in the body of the report. Management's formal comments are included in Appendix 3.

cc: Deputy Secretary
Under Secretary for Science and Energy
Assistant Secretary for Energy Efficiency and Renewable Energy
Chief of Staff
Chief Information Officer
General Counsel

SPECIAL REPORT ON THE OFFICE OF ENERGY EFFICIENCY AND RENEWABLE ENERGY'S INTEGRATED RESOURCE AND INFORMATION SYSTEM

TABLE OF CONTENTS

System Development, Cyber Security and Contracting Practices

Appendices

OFFICE OF ENERGY EFFICIENCY AND RENEWABLE ENERGY'S INTEGRATED RESOURCE AND INFORMATION SYSTEM

System Development, Cyber Security and Contracting Practices

The Office of Energy Efficiency and Renewable Energy (EERE) had not adequately managed the development and implementation of the Integrated Resource and Information System (IRIS). In particular, we determined that officials had not implemented effective project management practices when developing and implementing IRIS. EERE also had not implemented essential cyber security controls designed to protect the system and the information it contained. In addition, our review identified concerns related to contracting practices used to support the selection and procurement of IRIS components, including the purchase of software licenses and payments for labor to support development of the system.

Project Planning and Execution

EERE had not adequately managed the development of IRIS. Despite spending more than $7 million to date on the development and implementation of IRIS, we found that project planning and execution tools were not utilized to help ensure effective and efficient implementation of the project. In particular:

- Contrary to Federal and Department of Energy (Department) project management guidance, EERE officials had not developed an approved project execution plan with established baselines that contained detailed information related to the overall cost of the project, schedule for implementing milestones and the scope of IRIS functions. Absent a project execution plan, officials had not determined the total cost of the project and were unable to track expenditures against expected costs for the system development effort, a critical element to ensuring effective project management. In addition, although officials initially developed a project overview illustrating when they expected to implement 12 IRIS modules, they had not developed a detailed schedule for project implementation. EERE also had not developed an adequate cost/benefit and alternatives analysis prior to undertaking the IRIS project. Officials included a brief summary of potential advantages and disadvantages of utilizing existing systems to meet the program's needs as part of its *EERE Enterprise IT Solution Recommendations* document. However, we determined that the evaluation did not include a detailed review of which existing systems could meet users' needs or the potential costs of modifying existing systems. As noted by the Office of Management and Budget (OMB), one of the primary components of an appropriate analysis is determining whether existing resources can be modified to meet user needs. Subsequent to our review, EERE developed an approved Information Technology Services Office plan that incorporated milestones and estimates for cost and schedule for development of future IRIS modules through December 2014.

- Although the project was, in our view, a major information technology (IT) investment, EERE officials had not ensured that IRIS development efforts were supported by a capital asset plan even though development of a plan was recommended by EERE staff. According to OMB and Department guidance, including the Department's *Guide to IT*

Capital Planning and Investment Control issued in September 2010, a major IT investment is defined as an investment that has significant program or policy implications, high executive visibility and/or high development, operating or maintenance costs. The guidance states that such IT investments should be supported by a capital asset plan that includes information for sound planning, management and monitoring of the project. However, because EERE did not develop and submit a capital asset plan to the proper oversight organizations as part of project planning efforts, appropriate officials at OMB and the Department's Office of the Chief Information Officer were not aware of the project and could not provide adequate attention to ensure that the IRIS development was effectively managed. In addition to lack of visibility at a planning level, individuals told us, and this appeared to be supported by documentation reviewed, that EERE categorized funds being used for IRIS development as costs for other unrelated systems, thereby limiting transparency into the true cost of the project.

- Effective planning and identification of user requirements, activities that are intended to provide detailed metrics and increase the likelihood that the system will meet user needs, were not completed and resulted in significant changes to the scope of the project and acquisition of more software licenses than necessary. EERE intended IRIS to be implemented using a commercial-off-the-shelf (COTS) solution requiring only minimal modifications. However, we found that a lack of understanding of user requirements resulted in EERE spending significant funds for customization of the software. As part of the justification for selecting the chosen vendor as the supporting software application for IRIS, EERE officials estimated that labor costs of approximately $2.75 million would be required to place 12 IRIS modules into operation. However, subsequent to the acquisition of the software, officials diverted from the original plan and decided to customize the software by as much as 90 percent, in large part, because of user requests for changes to the COTS solution. As a result, EERE spent approximately $3.6 million for labor costs related to custom development and/or configuration of the COTS platform. Despite expending more than originally planned, the program had only placed 3 of the 12 planned modules into operation.

  In another example of ineffective planning, EERE anticipated a quick development and rollout of the IRIS project and purchased 1,000 software licenses at the beginning of the effort at a cost of about $1 million. However, we found that less than 200 licenses were used at the time of our review, which resulted in EERE paying about $675,000 for acquisition and maintenance of software licenses that were not utilized. A senior EERE official commented that the high number of software licenses was procured so that each EERE employee and external user would have their own license. However, without adequate project planning that included an analysis of when and how many licenses would be required, there was no basis to support the number of licenses purchased. Notably, prior to the acquisition of licenses for IRIS, certain EERE officials indicated that it would be easier to increase the number of licenses later rather than to decrease it. Furthermore, a contractor associated with the development of IRIS informed us that EERE should have discussed the number of licenses with the software vendor developers prior to procurement to determine the initial number of licenses needed. The same

official indicated that based on past experience, EERE could have bought only 50 licenses for development and testing until it was ready to deploy IRIS modules. Understanding user requirements early in the project can aid in the avoidance of re-work costs due to the lack of functionality and can remove a significant amount of guesswork in the planning stages. In response to our review, EERE significantly reduced the number of licenses maintained.

- Senior program officials regularly changed the scope and schedule for IRIS development efforts without fully appreciating and understanding the impacts to cost and operations. For example, management anticipated implementing all 12 IRIS modules by the first quarter of Fiscal Year (FY) 2014, and retiring 119 existing systems, resulting in estimated savings of nearly $1 million. However, only 3 of 12 modules had been implemented at the time of our review, and none of the 119 systems had been retired. While these were significant changes, there was no mechanism in place to formally approve the scope changes and related corrective actions to get the project back on track. We identified various other ad-hoc changes to IRIS that were not managed through a change control process, including one instance in which senior management reduced the number of modules to be implemented while at the same time extending the schedule. Subsequent to our review, EERE established a change control board in late December 2013. Our review of supporting documentation noted that the change control board was established to prioritize, approve, plan and integrate requests for changes to standard operating procedures. However, we found that the documentation lacked detailed information related to information system changes, such as what types of changes should be approved by a change control board and how the impacts of changes would be evaluated.

The issues identified previously are similar to those reported during our review of *Management Controls over the Development and Implementation of the Office of Energy Efficiency and Renewable Energy's Performance and Accountability for Grants in Energy System* (OAS-RA-10-14, July 2010). Although management concurred with our prior report recommendation to ensure that effective project management practices are implemented as part of system development and implementation efforts, the weaknesses discussed in our current report indicate that significant additional work is needed. Notably, EERE management told us that it reviewed prior Office of Inspector General (OIG) reports related to system development. In spite of this review, we noted that officials still did not ensure that actions taken in regard to IRIS were consistent with effective project management practices.

Cyber Security

EERE had not implemented essential cyber security controls designed to protect the IRIS system and the information it contained. We determined that even though the system was placed into operation, various cyber security controls had not been implemented. In particular:

- EERE placed one of the IRIS modules into operation without ensuring that the system met necessary cyber security requirements. Specifically, the module became operable in July 2013 even though it lacked completed documentation to demonstrate that

appropriate security controls were in place, including a risk assessment, system security plan, contingency plan and security controls assessment. In addition, while the system had been placed into operation, an authority to operate had not been granted by the responsible official. We noted that this was the second time the module was placed into operation without the necessary authority to operate. EERE initially placed this same module into operation in October 2012, but subsequently removed it from the network in February 2013, when it was discovered by program personnel that security requirements had not been considered and/or implemented. The authority to operate is important because it represents management's authorization to operate an information system and to explicitly accept the risk to organizational operations based on the implementation of an agreed-upon set of security controls.

- While an authority to operate was subsequently approved in August 2013, after the module was already in operation, we noted that important account management, audit log and configuration management controls still had not been addressed. Specifically, EERE support contractor tests of IRIS controls identified 34 failed controls, the vast majority of which were categorized as moderate risk failures. For instance, we noted numerous access control weaknesses continued to exist, including weaknesses related to user authorization and disablement and failure to implement password complexity rules in accordance with EERE policies. In addition, controls related to segregation of duties, multi-factor authentication for privileged users and mandatory security configuration management settings had not been implemented.

- When controls testing was performed, it was not always adequate to support the decision to authorize the system for operation. Contrary to National Institute of Standards and Technology (NIST) guidance, EERE's security assessment for the cloud computing software consisted primarily of online presentations and conference calls over a 2-day period and did not include detailed testing such as a vulnerability assessment. NIST states that a detailed review of existing controls should include not only interviews, but also the examination and testing of security controls implementation where applicable. In addition, EERE had not performed testing of security controls to be implemented by the cloud service provider such as controls related to access, account management and vulnerability scanning. In fact, officials were not permitted to retain security documentation from the vendor. As such, we were unable to fully evaluate the effectiveness of security over IRIS and determine whether additional controls should have been considered.

- EERE had not established and utilized separation of duties to ensure appropriate independence between individuals responsible for system security. NIST Special Publication 800-18, Rev. 1, *Guide for Developing Security Plans for Federal Information Systems*, states that the designated authorizing official, independent from the system owner, should approve the system for operation. However, we found that the authorizing official's supervisor was also the system owner, creating a conflict of interest and potentially resulting in pressure on the authorizing official to approve the system for operation even though controls were not adequately addressed. Our review of supporting

documentation and discussions with Federal and contractor personnel confirmed our opinion that there was a sense of pressure on the authorizing official to place the system into operation without fully implementing all security controls.

- Contrary to Federal requirements, EERE officials had not established a service level agreement with the cloud service provider prior to initiating use of the system. According to NIST, agencies must ensure that service level agreements legally bind a cloud provider, broker or carrier to implement all applicable security controls outlined in Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. In addition, the Federal Chief Information Officers Council notes that service level agreements are necessary between a cloud service provider and customer to contractually agree upon the acceptable service levels expected from the provider. Furthermore, the Federal Chief Information Officers Council noted that as a best practice, service level agreements should clearly define how performance such as response time, resolution/mitigation time and availability is guaranteed and require the providers to monitor service levels, provide timely notification of a failure to meet the service level agreements and evidence that problems have been resolved or mitigated.

As noted in numerous OIG reports, weaknesses related to the Department's cyber security program, including EERE's security program, unnecessarily increases the risk of compromise to the Department's information systems and can result in extensive and costly recovery efforts.

Contracting Concerns

Our review identified concerns related to contracting practices used to support the selection and procurement of IRIS components, including the purchase of software licenses and payments for labor to support development of the system. In addition, we noted instances of a senior EERE official inappropriately providing direction to contractor personnel. Specifically:

- We identified potentially troubling discrepancies related to activities that occurred during the selection of the COTS software that raised concerns regarding whether the process was carried out in an appropriate manner. For example, EERE did not select potential software applications using an open and competitive process. Although EERE officials conducted a preliminary analysis that allowed participants to analyze and evaluate three different solutions, including the chosen vendor, several participants we spoke with stated that the software options were not necessarily comparable. Furthermore, during our review, several officials stated that they believed the decision to use the selected COTS software was made prior to preliminary analysis being conducted. In preliminary comments on our report, management stated that it followed an acquisition process approved by the Department's Office of Management. For instance, management provided information to support that it obtained approval to acquire up to $2.5 million in IT purchases without competition. However, EERE's preliminary cost estimate for integration and related software licenses amounted to nearly $9 million through FY 2017. As such, we assert that the selection of software supporting the IRIS initiative was not fully competitive.

- In addition to the software application issues, we noted that rather than going through a competitive selection process, EERE management modified and utilized an existing Golden Field Office IT support services contract for the IRIS development effort. However, the IRIS efforts may have been outside the scope of work included in the support contract. Specifically, a new task was issued that was unrelated to the original contract task and essentially doubled the cost of the contract. In addition, the Statement of Work associated with the original contract indicated that activities were only to be performed at the Golden Field Office and not Headquarters, where nearly all of the IRIS work was conducted. Although EERE management noted that the contracting officer determined that the IRIS development work was within scope of the existing contract, we believe that a competitive selection process may have enhanced the Department's ability to lower development costs and improve the likelihood of project success.

- Contrary to Department acquisition guidance, a senior EERE official inappropriately directed work to IRIS contractors and subcontractors even though the official was not a contracting officer or representative. In one instance, we determined that the official demanded that a specific subcontractor employee be kept on the IRIS project, directing Federal and contractor staff to "Please ensure this happens…I will not accept anyone else." In another instance, the same official inappropriately directed a subcontractor how to bill work against existing funds.

Implementation of Requirements and Performance Monitoring

The issues identified were due, in large part, to an accelerated planning, development and deployment approach used by EERE officials to implement the IRIS project. In attempting to expedite the implementation of IRIS, program officials had not appropriately followed Federal requirements, Departmental guidance and best practices related to system development, cyber security and contract management. In addition, we determined that performance monitoring over the project was not adequate to help ensure its success.

Policies and Procedures

EERE had not effectively implemented policies, procedures and best practices related to project management to ensure that IRIS was developed and placed into operation on schedule and within budget. In addition, officials had not implemented Federal and Department cyber security requirements to ensure the system was operated in a secure manner. EERE officials also did not always follow established requirements related to contract management.

Department Order 415.1, *Information Technology Project Management*, directs that officials plan for implementation of IT projects using, among other things, project management plans, alternative analyses and requirements documents. Although EERE's preliminary comments to our report indicated that the program was not required to follow Department Order 415.1 because the life-cycle cost did not exceed $25 million, we determined that program officials had not identified the total life-cycle cost for IRIS, and preliminary estimates indicated that about $15 million would be spent in just the first 4 years of the project. In the absence of an adequate

cost/benefit analysis and detailed planning documentation, EERE could not ensure that the selected alternative met its needs in the most effective, economical and timely manner. EERE officials also had not ensured that they followed the Department's Capital Planning and Investment Control (CPIC) process – a process designed to help make certain that IT investments integrate strategic planning, budgeting, procurement and management in support of agency mission and business needs. Although required by the Department's *Guide to IT Capital Planning and Investment Control*, program officials did not develop detailed project management plans that included schedule milestones, project scope and cost information. Thus, EERE had no baselines against which to measure project success.

We also found that EERE had not effectively implemented Federal and Department requirements related to cyber security over IRIS. In particular, officials had not ensured that appropriate risk management controls were implemented related to the process for authorizing IRIS for operation. Specifically, contrary to NIST requirements for ensuring independence between the system owner and the authorizing official, we noted that EERE officials permitted the authorizing official to report directly to the system owner in a subordinate/supervisor capacity, creating a potential conflict of interest and lack of independence. Furthermore, program officials did not ensure that basic security controls were implemented such as the development and testing of system security plans.

EERE did not always follow established requirements for contract management. Specifically, it appears that officials ignored or lacked an understanding of the Federal Acquisition Regulation and Department guidelines regarding open competition and contract roles and responsibilities. For example, while the Federal Acquisition Regulation states that the contracting officers shall promote and provide for full and open competition in soliciting offers and awarding contracts, EERE officials did not use a fully competitive process to acquire the COTS software. EERE officials were unable to provide documentation to justify why full and open competition could not be used. Also, although the *Department of Energy Acquisition Guide* states that Federal managers must not direct a contractor to hire a particular individual, EERE officials we spoke with lacked an understanding of the various roles and responsibilities of those involved in communications with contractors outside of the scope of the contracting officer, contracting officer representative or task monitor.

Performance Monitoring

The lack of effective governance over the development effort resulted in confusion among team members regarding the direction of the project and precluded EERE from obtaining needed assistance from the Department's established IT management organization. Also, we identified various weaknesses related to performance monitoring of system development and implementation and related contracting practices. For instance, program officials had not always implemented monitoring practices that could have ensured that IRIS efforts were well-defined and changes were made in an organized manner.

EERE had not established a defined project governance structure to monitor performance, which caused confusion among project team members. Although roles and responsibilities were assigned in a draft project management plan, many Federal and contractor staff noted that they

were unsure of the chain of command and what was expected of them. Our review identified significant turnover of project managers for IRIS. Specifically, we identified at least five different officials who were delegated project manager responsibilities within a year or less. Best practices highlight that frequent turnover of key project personnel can detract from project success and contribute to an environment identified by confusion and low morale. In addition, EERE failed to follow the Department's existing governance structure for IT management by not reporting the project to the Office of the Chief Information Officer and the Department's Information Technology Council. This could have enabled the Department to maintain visibility over the status of the initiative's cost, schedule and technical baselines each quarter and help ensure the project was managed in an effective manner. While we noted that certain IRIS team members discussed the lack of CPIC compliance with EERE officials early in the project, no action was taken to ensure compliance with the Department's process.

In addition to management turnover, several officials commented that changes to the scope and overall direction of the project were not only being directed by the project manager but also from the various team leads who, in the opinion of one contractor, were working independently from one another. In addition, an official informed us that as the project progressed, a senior EERE official started to communicate directly with subcontractors instead of going through the project manager.

We also noted that, despite concerns raised by IRIS team members, EERE had not established and implemented a formal change control board to monitor and support project management and contract management decisions such as scope changes and changes to various contracts. Without a change control board, representatives from all EERE organizations that could be affected by the project were not always included in the decisions that could cause major impacts to mission work. Subsequent to our review and more than a year into the project, EERE recently established a change control board. However, the change control board was designed to focus on standard operating procedures, and the documentation supporting the organization was not specific in describing what types of system changes needed to go through the board or how the impacts of changes would be evaluated. Absent a well-defined governance structure, performance monitoring may not be effective and result in excessive costs and schedule delays caused by reversed or modified decisions from conflicting input of various stakeholders.

Other Matters

During our review, it became apparent that the work environment and morale within EERE may be significantly impacting program operations, including the IRIS development effort. Throughout the course of our review, we spoke with over 30 individuals from EERE Headquarters and the Golden Field Office, including Federal employees and support contractors. Staff stated they were discouraged from providing constructive feedback to management. Many individuals we spoke with also conveyed that they were pressured not to cooperate with the OIG and/or expressed fear of retaliation by management. For example:

- Personnel expressed concern that EERE Headquarters management had asked employees to not be transparent to the OIG. During a meeting held near the end of our site visit at the Golden Field Office, we were notified by several individuals that EERE Headquarters

management told personnel not to say anything negative to the OIG regarding the software product selected. These individuals noted that this deeply concerned them because during past audits, they had always been encouraged by other management officials to speak openly to the OIG.

- During the course of our interviews, several people expressed fear that EERE Headquarters management would know they talked to the OIG. For instance, one person refused to record their attendance at a meeting out of fear of retaliatory action by management. Several other individuals expressed concern that EERE Headquarters management would know who had spoken to the OIG based on what was published in our report. Whether real or perceived, the fear of cooperating with the OIG reflected an environment where individuals did not believe they were always free to express concerns regarding potential fraud, waste and abuse.

- We were told by numerous individuals that senior EERE officials did not support constructive feedback. For instance, one person described the work environment as "oppressive" and said that "yes, sir" was expected and feedback was not welcome. Other individuals informed us that a senior EERE official did not value the expertise of his employees and suggested that employees were reassigned if they presented opinions that contradicted the senior official. Furthermore, an official noted that if concerns were raised to management, the individuals became accused of being resistant to change.

Although we only highlighted a few examples, many individuals expressed similar concerns with senior EERE leadership. Despite the actions of EERE management and the environment within the office, the vast majority of EERE staff members we interviewed and/or sought data from ultimately cooperated. And, we did not observe any overt actions to impede our review of allegations made against EERE pertaining to the IRIS project. However, given the concerns reported to us, we cannot determine with certainty whether we had full access to the full range of critical project information.

Impact and Path Forward

Lacking an adequate cost/benefit and alternatives analysis prior to the development of the IRIS project, the Department could not ensure that the selected alternative met its needs in the most effective, economical and timely manner. Also, absent a well-defined schedule, scope and budget that includes established baselines and deliverables, EERE runs a higher than necessary risk of cost overruns and schedule delays for future IT developments, including the development of future IRIS modules. In addition, without the submission of a capital asset plan, the project may not be transparent to Department and other Federal oversight officials and may not receive the necessary attention to ensure that the project is successfully completed. Furthermore, not adhering to existing contracting policies and procedures for open competition may result in the Department paying higher than necessary costs for the implementation of IRIS. Moreover, without improvements to the work environment and morale within EERE, the IRIS development effort, as well as program operations, in general, will continue to be adversely impacted.
In light of the growing number of security threats to the Department, including the recent compromise of current and former employees' personally identifiable information, programs

must take into consideration and mitigate potential cyber security risks that may have an adverse impact on the Department's systems and information. By introducing systems that have not completed the necessary risk management framework, including detailed testing of cyber security controls, the Department runs an increased risk that weaknesses within the systems being deployed could be exploited by an individual with malicious intent. In addition, the lack of a service level agreement between EERE and its software vendors may not allow the Department to pursue legal penalties or compensation for unacceptable performance levels or security non-compliance.

RECOMMENDATIONS

To more effectively manage its system development efforts, we recommend that the Deputy Under Secretary for Science and Energy:

1. Consider suspending the IRIS project until program officials develop and implement effective project management and cyber security practices.

2. Ensure that project management controls are in place prior to proceeding with the IRIS initiative, including:

    a) Finalization of project management plans that includes detailed costs, scope and schedules to support the project;

    b) Development of cost/benefit and gap analyses, and review of the project by the Department's Information Technology Council; and

    c) Development of a capital asset plan and related reporting to the Office of Management and Budget.

3. Implement necessary cyber security requirements for IRIS to ensure that it is secure to operate and adequately protects the Department's systems and information, including establishing service level agreements, as appropriate.

4. Ensure that all EERE employees implement appropriate contract management practices, including competitive selection and appropriate contact between Federal and contractor employees.

5. Perform an evaluation to determine whether the development contract for IRIS was adequately competed/fully competitive.

6. Ensure that officials are aware of their duty to cooperate with the Office of Inspector General as outlined in Department orders through training, outreach or other activities, as appropriate.

7. Conduct an independent review of personnel matters within EERE to determine the extent of personnel management weaknesses and take any necessary disciplinary actions against individuals responsible for weaknesses identified.

MANAGEMENT REACTION

Management concurred with the report's recommendations and indicated that corrective actions were initiated and/or planned to address the issues identified. For instance, management requested that independent fact finding analyses be completed related to IT project management including cyber security, acquisition and contract management and other matters related to the workforce environment. Management noted that it will evaluate whether or not the actions taken by EERE with respect to the IRIS project are sufficient to allow the project to continue in a limited manner or whether it should be immediately suspended. Management commented that the project's cyber security implementation and contract management practices will also be reviewed to identify the underlying causes of weaknesses identified in our report.

Management indicated that it was taking immediate steps to reassure all employees of their duty to cooperate with the OIG. Management commented that the Department will conduct an independent analysis to determine the extent of personnel management weaknesses and will work to identify appropriate actions, including any necessary disciplinary actions against individuals responsible for weaknesses identified.

AUDITOR COMMENTS

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

Appendix 1

OBJECTIVE

To determine whether the Integrated Resource and Information System development effort was effectively managed by the Office of Energy Efficiency and Renewable Energy.

SCOPE

The audit was performed between July 2013 and April 2014 at the Office of Energy Efficiency and Renewable Energy Headquarters in Washington, DC, and the Golden Field Office in Golden, Colorado. The audit was conducted under Office of Inspector General Project Number A13TG049.

METHODOLOGY

To accomplish our objective, we:

- Reviewed applicable laws and regulations pertaining to system development, Federal acquisitions and cyber security;
- Reviewed applicable standards and guidance issued by the Office of Management and Budget;
- Reviewed prior reports issued by the Office of Inspector General;
- Held discussions with program officials and contractor personnel from Department of Energy Headquarters and the Golden Field Office; and
- Reviewed available documentation related to the Energy Efficiency and Renewable Energy's Integrated Resource and Information System project, including project management, cyber security and contract documents.

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 of Energy's implementation of the *GPRA Modernization Act of 2010* and determined that Energy Efficiency and Renewable Energy had not established performance measures for system development. Because our review was limited, it would not have necessarily disclosed all internal control deficiencies that may have existed at the time of our evaluation. We did not rely on computer-processed data to satisfy our objectives.

An exit conference was held on April 2, 2014.

PRIOR REPORTS

- Audit Report on *Naval Reactors Information Technology System Development Efforts* (DOE/IG-0879, December 2012). The audit found that the Naval Reactors Program had taken a number of positive actions designed to resolve development issues associated with the Enterprise Business System (EBS). However, our review identified continuing system development issues. In particular, neither Naval Reactors officials nor the project contractors had adequately considered the use of a commercial-off-the-shelf product prior to upgrading and modernizing the financial components of EBS. In addition, we found that Naval Reactors had encountered delays in the EBS development effort, resulting in additional costs and a later than expected completion date; and, we found that the EBS project had not been reported to the Department of Energy and the Office of Management and Budget as a major information technology investment, as required. Despite spending approximately $10 million of the budgeted $12.8 million for the procurement phase of the EBS development effort, officials had not submitted the required budgetary information to the Department of Energy or Office of Management and Budget, an action that could have allowed for improved performance monitoring.

- Audit Report on *Management Controls over the Development and Implementation of the Office of Energy Efficiency and Renewable Energy's Performance and Accountability for Grants in Energy System* (OAS-RA-10-14, July 2010). We found that although the Office of Energy Efficiency and Renewable Energy's Performance Accountability for Grants in Energy (PAGE) System had been partially deployed and was being used by Energy Efficiency and Renewable Energy and grant recipients, it did not satisfy a number of important cyber security requirements. In addition, the deployment was not performed in accordance with Federal requirements. Specifically, the audit found that PAGE was placed into operation even though cyber security planning and testing was not completed, and basic project management practices were not followed during planning, development and implementation of PAGE. In particular, cost and schedule baselines were not created to help manage the project, and officials had not fully considered alternatives to a custom system development, practices which are designed to increase the efficiency of system development.

- Audit Report on *Management Controls over the Department's WinSAGA System for Energy Grants Management Under the Recovery Act* (OAS-RA-10-05, March 2010). We found that certain security concerns with the system could increase the risk of compromise of grant data. Specifically, controls over system access were not appropriate, including assigning excessive user access privileges and inadequate password complexity. In addition, appropriate system backup and recovery procedures had not been implemented, including the storage of sensitive system information in an unsecured location and insufficient testing to ensure that the system could be restored in the event of a disruption. Further, security planning documentation and control testing were incomplete and contained several inconsistencies.

Department of Energy
Washington, DC 20585

March 26, 2014

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

FROM: DR. MICHAEL L. KNOTEK
DEPUTY UNDER SECRETARY
OFFICE OF THE UNDER SECRETARY FOR SCIENCE AND ENERGY

SUBJECT: Response to Office of Inspector General Draft Special Report on "Office of Energy Efficiency and Renewable Energy's Integrated Resource and Information System"

The Office of the Under Secretary for Science and Energy (S4) appreciates the opportunity to respond to the Office of Inspector General's (OIG) draft report. S4 concurs with all seven recommendations and has taken initial steps to address the issues raised in the report. Additionally, S4 will continue with appropriate follow on actions, as described below.

In April 2012, the Office of Energy Efficiency and Renewable Energy (EERE) initiated a broad overhaul of its organization, management, and operations in order to achieve greater efficiency and enable better stewardship of taxpayer dollars. The Integrated Resource and Information System (IRIS) represents the information technology (IT) portion of these efforts. As noted in the Office of the Inspector General's (OIG) report, EERE began development of IRIS with the aim of consolidating over 100 existing IT systems into a single, integrated, cloud-based, and mobile-ready Enterprise IT solution. IRIS is intended to be EERE's project management platform, designed to facilitate real-time analysis and leadership visibility of EERE's programs and projects by tracking milestones and financial outlays across the enterprise. IRIS is also intended to enable online collaboration across EERE and with external partners.

The Department of Energy takes seriously its commitment to taxpayer interests and the integrity of its programs. S4 now understands that the IRIS initiative was not conducted in a manner consistent with the Department's typical processes and accompanying high standards for IT project management, cyber security and contract management. Considering the taxpayer resources already spent on this initiative, we are committed to the expeditious resolution of the issues identified by the OIG and the determination of the appropriate path forward for IRIS.

While all of the allegations in the report are troubling, of particular concern are allegations of withholding information or otherwise discouraging frank and open cooperation with the OIG.

The Department is committed to fostering a work environment in which everyone feels free to ask questions and raise concerns without fear of reprisal. Immediate actions will be taken to reassure all employees working within programs reporting to S4 that cooperation with the OIG is a key duty of their jobs that cannot and shall not be encroached upon for any reason.

The OIG's report identifies concerns in three primary areas: IT project management (including cyber security), acquisition and contract management, and other matters tied to the workforce environment. S4 has requested fact finding analyses, independent of the EERE organization, to be completed in each of these areas. The analysis teams will be comprised of subject matter experts from appropriate Departmental elements, including, but are not limited to, the Office of Management (MA), the Office of the Chief Information Officer (OCIO), the Office of Hearings and Appeals (OHA), and the Office of the General Counsel (GC). The ultimate goal of these three fact finding efforts is to determine the details surrounding the issues in the report, the underlying cause(s), and specific recommendations for corrective action.

Since the OIG initiated its inquiry in July 2013, EERE has taken steps to strengthen its oversight, planning and management of the IRIS project, and has formally briefed the DOE Information Technology Council on IRIS activities. EERE has also reached out to other Federal agencies to examine possibilities for leveraging investments in application development and sharing best practices and lessons learned. These steps will be examined within the fact finding analyses to determine their contribution to resolving the issues identified in the OIG's report.

Specific responses to OIG recommendations are provided below.

RECOMMENDATION #1: *Consider suspending the IRIS project until program officials develop and implement effective project management and cyber security practices.*

MANAGEMENT RESPONSE: CONCUR. The Department is committed to effective project management and compliance with cyber security protocols. As described in the report, EERE has addressed some of the issues related to project management and cyber security practices. S4 has consulted with the OCIO to determine whether these actions are sufficient to permit the IRIS project to continue in a limited manner, or whether it should be immediately suspended pending the outcome of an independent fact finding analysis on the overall conduct of the project. All appropriate actions associated with this recommendation will be implemented by April 15, 2014.

RECOMMENDATION #2: *Ensure that project management controls are in place prior to proceeding with the IRIS initiative, including: (a) Finalization of project management plans that includes detailed costs, scope and schedules to support the project; (b) Development of cost/benefit and gap analyses, and review of the project by the Department's Information Technology Council; and (c) Development of a capital asset plan and related reporting to the Office of Management and Budget.*

MANAGEMENT RESPONSE: CONCUR. The Department is committed to effective project management, and will act swiftly to address the issues identified in the report. S4 will rely upon the findings and recommendations of its independent fact finding analysis of EERE's IT project management to ensure that all appropriate controls are in place and working, indicating that IRIS

is on the appropriate path moving forward. All appropriate actions associated with this recommendation will be implemented by June 30, 2014.

RECOMMENDATION #3: *Implement necessary cyber security requirements for IRIS to ensure that it is secure to operate and adequately protects the Department's systems and information, including establishing service level agreements, as appropriate.*

MANAGEMENT RESPONSE: CONCUR. The development and deployment of any Departmental IT system must comply with all cyber security protocols and requirements. While appropriate Departmental guidance exists in this area, it was apparently not followed initially in this instance. S4 will rely upon the findings and recommendations of its independent fact finding analysis to identify the appropriate steps that must be taken to protect the Department's systems and information handled within IRIS, and to identify the underlying causes of initial shortfalls in the execution of cyber security requirements. All appropriate actions associated with this recommendation will be implemented by June 30, 2014.

RECOMMENDATION #4: *Ensure that all EERE employees implement appropriate contract management practices, including competitive selection and appropriate contact between Federal and contractor employees.*

MANAGEMENT RESPONSE: CONCUR. The Department is committed to strict adherence to procurement rules and procedures. S4 will rely upon the findings and recommendations of its independent fact finding analysis to identify the appropriate steps that must be taken to ensure appropriate contract management practices. All appropriate actions associated with this recommendation will be implemented by June 30, 2014.

RECOMMENDATION #5: *Perform an evaluation to determine whether the development contract for IRIS was adequately competed/fully competitive.*

MANAGEMENT RESPONSE: CONCUR. The Department is committed to strict adherence to procurement rules and procedures. The independent fact finding analysis of acquisition and contract management will include an evaluation of whether the development contract for IRIS was placed in accordance with competition rules. All appropriate actions associated with this recommendation will be implemented by May 31, 2014.

RECOMMENDATION #6: *Ensure that officials are aware of their duty to cooperate with the Office of Inspector General as outlined in Department of Energy Orders through training, outreach or other activities, as appropriate.*

MANAGEMENT RESPONSE: CONCUR. Frank and open cooperation with the Inspector General is absolutely essential to ensuring that Departmental activities are appropriately conducted. S4 will take immediate steps to ensure that all employees under the purview of S4 are aware of their duty to cooperate with the OIG through a variety of activities, including distribution and active discussion of DOE Order 221.2A, "Cooperation with the Office of Inspector General," as well as other appropriate materials determined by S4 in concert with the

OIG and the Department's Office of the General Counsel (GC). All appropriate actions associated with this recommendation will be implemented by April 30, 2014.

RECOMMENDATION #7: *Conduct an independent review of personnel matters within EERE to determine the extent of personnel management weaknesses and take any necessary disciplinary actions against individuals responsible for weaknesses identified.*

MANAGEMENT RESPONSE: CONCUR. The Department's Office of Hearings and Appeals will conduct an independent fact finding analysis within EERE to determine the extent of personnel management weaknesses that may have contributed to the conduct of the IRIS project and subsequent OIG review. Based on the outcome of this review, S4 will work with the Office of the General Counsel and the Office of the Chief Human Capital Officer (OCHCO) to determine appropriate actions, including any necessary and appropriate disciplinary actions against individuals responsible for weaknesses identified. In the interim, S4 has directed EERE leadership to refrain from major personnel actions without further guidance from S4, the Office of the Chief Human Capital Officer, and the GC. The fact finding associated with this recommendation will be completed by June 30, 2014. Once the fact finding is reviewed, any appropriate disciplinary actions will be taken.

If you have any questions, please contact Patrick N. Holman at (202) 586-7016.

IG Report No. DOE/IG-0905

CUSTOMER RESPONSE FORM

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

1. What additional background information about the selection, scheduling, scope, or procedures of the audit or inspection would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in the report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report that would have been helpful?

5. Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

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

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

ATTN: Customer Relations

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

This page intentionally left blank.

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

U.S. Department of Energy Office of Inspector General Home Page

http://energy.gov/ig

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