U.S. Department of Energy
Office of Inspector General
Office of Audit Services

Audit Report

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

Department of Energy
Washington, DC 20585

July 22, 2010

MEMORANDUM FOR THE ASSISTANT SECRETARY, ENERGY EFFICIENCY AND RENEWABLE ENERGY

FROM: Rickey R. Hass
Deputy Inspector General
for Audit Services
Office of Inspector General

SUBJECT: INFORMATION: 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"

BACKGROUND

As a result of the American Recovery and Reinvestment Act of 2009 (Recovery Act), the Department of Energy (Department) received $3.2 billion for grants to states, territories, local governments, and Indian tribes under the Energy Efficiency and Conservation Block Grant (Block Grant) Program. To help manage and track block grants, the Department's Office of Energy Efficiency and Renewable Energy (EERE) plans to spend approximately $9.5 million, nearly all of which is Recovery Act funding, for development and operation of the web-based Performance and Accountability for Grants in Energy (PAGE) System. PAGE began limited operation in September 2009 and was utilized by Block Grant recipients for quarterly Recovery Act reporting beginning in October 2009. PAGE will also replace the Windows System Approach to Grants Administration (WinSAGA) legacy system for tracking grant recipients' performance under the State Energy and Weatherization Assistance Programs, programs that received a combined $8.1 billion through the Recovery Act.

Our report on *Management Controls over the Department's WinSAGA System for Energy Grants Management Under the Recovery Act* (OAS-RA-10-05, March 2010), found that the system suffered from a number of security and operations management issues. These weaknesses had the potential to impact PAGE since it was to be developed by the same contractor and managed in a manner similar to WinSAGA. Because of the importance of the system to managing the EERE grant programs, we initiated this audit to determine whether PAGE was developed and implemented in accordance with Department and Federal cyber security and project management requirements.

RESULTS OF AUDIT

Although PAGE had been partially deployed and was being used by EERE and grant recipients, it did not satisfy a number of important cyber security requirements. In addition, the

development of the system was not performed in accordance with Federal requirements. Specifically:

- PAGE was placed into operation even though cyber security planning and testing was not completed. As a consequence, the system suffered from weaknesses related to inadequate risk assessments and problems with access controls, each of which could increase the risk of compromise; 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.

These issues were due, in large part, to the accelerated planning, development and deployment approach adopted by the Department. Because of a need to quickly deploy the system, officials elected to proceed without completing all required cyber security planning, assessment, and security testing. The desire to quickly deploy the system also contributed to the decision to not complete various Office of Management and Budget required project management activities prior to moving forward with development. EERE's decisions to not perform these cyber security and project management tasks placed the PAGE system and the network on which it resides at increased risk that the confidentiality, integrity, and availability of the Department's information systems and data could be compromised. In addition, the program may spend more than necessary for development and implementation activities.

We understand the importance of ensuring the availability of a system for managing EERE's grant programs and the short timeframe that was available for system development and implementation. However, there is an equally pressing need to ensure that systems, and the corporate networks on which they reside, are not exposed to higher than necessary risk of compromise. While EERE officials took action to address a number of the technical cyber security weaknesses we identified during our system vulnerability and penetration testing, additional action is necessary to resolve security problems and prevent future development issues. For that reason, we made several recommendations which, if fully implemented, should help improve future system development efforts and enhance the Department's cyber security posture.

MANAGEMENT REACTION

Management generally concurred with the recommendations in the report and indicated that corrective actions were underway to address our recommendations. Management's comments are included in Appendix 3.

Attachment

cc: Deputy Secretary
Under Secretary of Energy
Chief of Staff
Chief Financial Officer
Acting Chief Information Officer

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

TABLE OF CONTENTS

Cyber Security and System Development

Appendices

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

Cyber Security and System Development

We found that the Performance and Accountability for Grants in Energy (PAGE) system did not satisfy various Federal and Department of Energy (Department) cyber security and project management requirements. Specifically, significant weaknesses related to security planning and testing and access controls were identified that, if not fully addressed, could result in a higher than necessary cyber security risk. In addition, program officials had not ensured that fundamental project management practices required by the Office of Management and Budget (OMB) for this type of development, such as business process reengineering and development of cost and schedule baselines, were followed when deciding to develop and implement PAGE.

System Security

Office of Energy Efficiency and Renewable Energy (EERE) officials initiated operation of PAGE without ensuring that the system met necessary cyber security requirements. The National Institute of Standards and Technology (NIST) requires that a risk management framework be applied to Federal information systems prior to them being placed into operation. Through this process, systems undergo testing to ensure that minimum security controls are implemented correctly, operating as intended, and producing the desired outcome. Following testing, the program's Authorizing Official is responsible for allowing operation of the system by accepting any residual risks. In addition, the Under Secretary of Energy Program Cyber Security Plan (Energy PCSP) – to which PAGE is subject – requires that all systems complete this process prior to processing live data or information.

In spite of these requirements, we found that PAGE began operation in September 2009 even though the system authorization process had not yet been completed. Required security documentation such as a risk assessment, system security plan, and contingency plan had not been developed; security controls had not been tested; and PAGE had not been approved to operate by the Authorizing Official. For instance, the document detailing the controls that should have been implemented was not finalized until January 2010. Because the system's controls had not been fully documented, an independent security assessment could not be performed to confirm implementation. The system's implementation

timeline indicated that these tasks were planned as part of the next phase of implementation, which was scheduled for completion in May 2010 – eight months after the system initially became operational. Ensuring these tasks were performed was critical because the system is a web-based application with almost 2,500 users. Since it is connected to the Internet, its compromise could cause significant damage to the Department's networks.

Near the end of our audit, PAGE was given an interim authority to operate even though the security assessment – a major component of NIST's Risk Management Framework – still had not been completed. NIST requires that, when requesting authority to operate a system, a complete authorization package – consisting of the system security plan, the results of security control testing, and the Plan of Action and Milestones (POA&M) for tracking corrective actions – must be presented to the Authorizing Official. This documentation provides information needed to make credible risk-based decisions regarding whether to authorize operation of the system. However, an independent security assessment had not been completed and was not scheduled until May 2010.

In commenting on our draft report, management stated that this testing started in late June 2010 and was expected to be completed by the end of September 2010 – four months later than initially anticipated and a year after the system became operational. We also noted that the POA&M listed several critical areas where the controls that were documented in the system security plan had not been implemented. These included controls in the areas of system access, configuration management, and contingency planning and recovery. Our review of the system security plan confirmed that 34 percent of the controls required by NIST had not been implemented for the PAGE system. Furthermore, documentation provided by the program disclosed that cyber security had not been incorporated into the system development process for PAGE.

To support our review of system security, we performed vulnerability scanning and penetration testing on PAGE and noted several additional weaknesses related to access controls for the system. Specifically, we identified weaknesses with password management and hardware configurations. We also identified multiple vulnerabilities within the PAGE web interface that could have allowed an unauthorized individual access to the system or the ability to use the system as an

intermediary for other attacks. As noted in our report on *Management Controls over the Department's WinSAGA System for Energy Grants Management Under the Recovery Act* (OAS-RA-10-05, March 2010), and our report on *Management of the Department's Publicly Accessible Websites* (DOE/IG-0789, March 2008), web-based applications are particularly vulnerable to exploit. Had program officials completed security testing of PAGE prior to its operation, they could have identified and addressed many of the weaknesses we noted. Following discussion of the results of our testing, EERE management took action to correct most of the technical issues identified.

System Development

The development of PAGE was not planned to ensure that the most cost-effective system was selected for implementation. Specifically, required analyses were not always completed and EERE officials did not fully consider existing systems and commercial-off-the-shelf software. The OMB requires that agencies initiate the acquisition of new information technology (IT) assets only when no existing alternative can meet the need; simplify or otherwise redesign work processes to reduce costs; and reduce project risk by avoiding custom designed components and ensuring involvement and support of users in the design and testing of the asset. In addition, the Federal Acquisition Regulation requires that agencies perform acquisition planning and conduct market research for all acquisitions to ensure that the most suitable approach to the acquisition is utilized.

We found that when planning to replace the aging Windows System Approach to Grants Administration (WinSAGA) system, EERE officials did not adequately research and evaluate potential alternatives, including the use of existing Department systems or acquisition and modification of commercial-off-the-shelf software prior to beginning development activities. Specifically, a gap analysis, completed in December 2008, recommended that EERE develop a web-based application as soon as possible, noting that this recommendation was the most cost-effective alternative. While the development of PAGE began in March 2009, program officials did not complete an alternatives analysis until three months later. Even after this analysis had been completed, it did not include a determination of whether other Department elements had existing systems that would meet

EERE's need, and was based on cost data that was more than two years old. In commenting on our draft report, management noted that much of the critical portions of an alternatives analysis were underway by February 2009. However, our review of documentation provided to support this assertion found that, while it identified the information needs for a new system, it did not provide information regarding development alternatives. Furthermore, contracting officials were unable to provide documentation related to acquisition planning or market research that may have been performed prior to soliciting vendors to develop PAGE. As a result, the Department could not ensure that the selected alternative met its needs in the most effective, economical and timely manner. The need for effective project management is further highlighted because development and maintenance of PAGE was mostly funded through the American Recovery and Reinvestment Act of 2009 (Recovery Act), which stressed the need for accountability of government programs and operations.

We also determined that detailed cost and schedule baselines designed to aid management with oversight of the PAGE project were not developed. Without such information, management was unable to adequately track the timing and expenditure of funds for the system development effort. As part of its quarterly reporting responsibilities to the Department's Chief Information Officer, EERE disclosed, in October 2009, that PAGE was on-time and within budget and gave it a score of "green" on its IT Council Scorecard. However, we found that the overall project completion date had slipped three months. In addition, EERE officials were unable to provide a detailed cost baseline for the development of PAGE. Without this information, they would have been unable to determine whether or not the project was within budget.

Security Monitoring and Project Management

These issues were due, in large part, to the accelerated planning, development and deployment approach adopted by the Department. Because of a need to quickly deploy the system, officials elected to proceed without completing all required cyber security planning, assessment, and security testing. The desire to quickly deploy the system also contributed to the decision to not complete various OMB required project management activities prior to moving forward with development.

Security Monitoring

Program officials had not taken an effective risk-based approach to ensure that cyber security requirements necessary for protecting the PAGE system and the information it contained were in place prior to operation of the system. In particular, officials stressed the need to place the system into operation over ensuring that cyber security requirements were met. In addition, EERE had not established an adequate cyber security program management structure designed to help with implementation of an effective cyber security posture.

Although the Energy PCSP required that the system owner obtain the proper authorization based on risk prior to starting system operations, program officials commented that the need to quickly place the system into operation outweighed the need for sufficient evaluation and implementation of security controls. While we recognize the need for EERE to implement the PAGE system in a prompt manner, incorporating security controls and assessing their adequacy during development would not have necessarily delayed the system deployment, but would have helped to ensure a secure computing environment. In addition, EERE had not ensured that an appropriate management structure was in place over the cyber security program to make risk-based decisions as part of system implementation.

PAGE was placed into operation even though a formal evaluation of security risks and vulnerabilities was not prepared for the authorizing official – the individual responsible for accepting the risk of a system's operation. In addition, even though the Energy PCSP required that an authorizing official with system oversight be appointed in writing by the Under Secretary of Energy or the Assistant Secretary for EERE and receive training specific to their role and responsibilities, no one with the appropriate level of authority was appointed to this position at the time the system was placed into operation. This was of particular concern regarding PAGE because, at the time it became operational, minimum security controls had not been fully implemented on the system and performance of those controls had not been assessed.

Project Management Practices

When planning for the development and implementation of PAGE, EERE officials had not ensured that required system development and project management practices for major IT investments were followed. Due to time limitations, program officials directed that the development of PAGE begin without performing the necessary analyses. Specifically, the initial recommendation of the gap analysis conducted when deciding to replace WinSAGA was to review commercial-off-the-shelf, government-off-the-shelf, and existing Department systems, and then perform the required cost-benefit analysis that would include developing a web-based application. However, officials did not follow through with this recommendation because they believed the process would take too long and instead decided to immediately begin development of the web-based application, PAGE. In addition, EERE officials commented that they did not seek input from grant recipients – the system's external users – related to the design of PAGE due to the limited time before the system had to be operational. While we realize that the program faced constraints which reduced the amount of time available to develop the system, we noted that obtaining user input at the beginning of a system development effort such as PAGE significantly increases the likelihood that the system will meet user needs. A proactive approach such as this can also aid in the avoidance of re-work costs due to a lack of functionality.

Risk to Systems and Sensitive Information

Without improvements to EERE's cyber security and project management practices, PAGE may introduce higher than necessary risks to the Department's information systems. Future EERE development projects could also cost more than necessary. In particular, the cyber security weaknesses identified during our review could have resulted in compromises to the Department's IT infrastructure had they been exploited by an individual with nefarious intent. For instance, our testing revealed that the ability existed to gain unauthorized administrative access to the system. This included the ability of authorized users to inappropriately elevate their own access privileges. In addition, without having adequately tested the system security controls for PAGE, program officials were unable to effectively ensure that the system and the network it resided on could be protected when it became operational. The lack of a contingency plan also increased the risk that the Department and other users of

the PAGE system could not effectively continue relevant operations in the event of a significant system outage.

The project management issues we identified may result in the Department spending more than necessary for a custom-built system when other less expensive, viable alternatives may have been available. This particular situation could have been avoided had the appropriate levels of acquisition planning and market research been conducted. For example, had a cost estimate been developed and used during the solicitation review process, EERE may have been able to make more efficient use of Recovery Act funds. During a time of increased attention to transparency of government spending, it is important that the Department's programs perform the required analyses before funds are expended to ensure that the government is receiving the most benefit from its expenditure of the taxpayers' money.

RECOMMENDATIONS

To help improve the effectiveness of cyber security and system development efforts, we recommend that the Assistant Secretary for Energy Efficiency and Renewable Energy ensure that:

1. A risk-based approach is taken when developing and implementing information systems, including review of development and implementation efforts at the appropriate management level;

2. Appropriate security protection measures over the PAGE system are implemented and tested using a risk-based approach in the most expeditious manner possible; and,

3. Effective project management practices are implemented as part of ongoing and future development efforts for IT systems, to include evaluation of viable alternatives, completion of detailed cost and alternatives analyses, acquisition planning, and market research prior to making funding decisions.

MANAGEMENT REACTION

EERE management generally concurred with the recommendations in our report. In addition, management indicated that corrective actions were underway to address the recommendations. Management also provided clarification regarding its actions as they related to our recommendations.

In particular, management commented that, while seeking to mitigate risk, it was also necessary to accommodate compressed timelines imposed by the Recovery Act and ensure cost-effectiveness in conducting system security activities on PAGE. Management stated that the approach utilized to authorize the PAGE system for operation allowed EERE to achieve a cost-balanced and risk-based approach by performing all steps required by NIST after major phases of the system's development. Management noted that this tailoring was acceptable and in accordance with NIST Special Publication (SP) 800-30, *Risk Management Guide for Information Technology Systems.*

In addition, management recognized the need for effective management practices as part of ongoing and future IT development efforts. However, management noted that, in the case of PAGE, a compressed deployment timeline was necessary to meet the goals of the Recovery Act. Furthermore, management disclosed that independent security control testing on the PAGE system began in June 2010 and was expected to be completed by the end September 2010. Management indicated that the results of this testing will be used to define the system's residual risk.

AUDITORS COMMENTS

Management's comments are generally responsive to our recommendations. Where appropriate, we made changes to the body of the report to address management's comments. We agree that cost and risk are significant factors that should be considered when deciding to operate an information system. We also agree that it was necessary to expedite development and implementation of the PAGE system to aid in Recovery Act activities. However, NIST requires that an assessment of security controls be conducted and the resulting assessment report be presented to the Authorizing Official for use in making the decision to allow the system to operate. As noted in our report, PAGE was permitted to operate even though testing of controls is not expected to be completed until September 2010 – limiting the usefulness of planned risk assessments. Management's comments are included in Appendix 3.

Appendix 1

OBJECTIVE

To determine whether the Performance and Accountability for Grants in Energy (PAGE) system was developed and implemented in accordance with Department of Energy (Department) and Federal cyber security and project management requirements.

SCOPE

The audit was performed between November 2009 and May 2010 at Department Headquarters in Washington, DC.

METHODOLOGY

To accomplish our objective, we:

- Reviewed applicable laws and Department directives, including those pertaining to information system security and project acquisition planning;
- Reviewed applicable standards and guidance issued by the Office of Management and Budget related to system development;
- Reviewed prior reports by the Office of Inspector General and the Government Accountability Office;
- Obtained documentation from and held discussions with officials from the Department's Office of Energy Efficiency and Renewable Energy (EERE) and contractor personnel relating to system security and controls and system development efforts; and,
- Analyzed system documentation to determine whether the risks of operating PAGE had been identified and addressed before the system was allowed to operate.

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 finding and conclusions based on our audit objectives. Accordingly, we assessed significant internal controls and EERE's implementation of the *Government Performance and Results Act of 1993* and determined that it had established performance measures for management and operation of its grant management systems. 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 rely on computer-processed data, to some extent, to satisfy our objective related to system security. In this case, we verified our findings using manual techniques.

An exit conference was held with Department officials on July 20, 2010.

RELATED REPORTS

- *Management Controls over the Department's WinSAGA System for Energy Grants Management Under the Recovery Act* (OAS-RA-10-05, March 2010). The audit found that the Windows System Approach to Grants Administration (WinSAGA), as currently configured, appeared to be capable of processing the additional formula grant transactions resulting from the American Recovery and Reinvestment Act of 2009 (Recovery Act). However, the audit did identify certain security concerns with the system that could increase the risk of compromise of grant data. Specifically, controls over system access had not always been implemented as required; appropriate system backup and recovery procedures had not been implemented; and, security planning documentation and control testing were incomplete and contained several inconsistencies. The issues we identified were due, at least in part, to inadequate communication and implementation of required cyber security policies by Headquarters and state officials. While no evidence of compromise was found, without improvement WinSAGA, and the information it maintains, could be exposed to a higher than necessary level of risk of compromise, loss, modification, and non-availability.

- *Department of Energy's Efforts to Meet Accountability and Performance Reporting Objectives of the American Recovery and Reinvestment Act* (OAS-RA-09-04, September 2009). The Department of Energy's (Department) efforts to develop, refine, and apply the control structure needed to ensure accurate, timely, and reliable reporting to be both proactive and positive. The audit did, however, identify certain issues relating to Recovery Act performance management, accounting and reporting accuracy, and timeliness that should be addressed and resolved. In particular, program officials had not yet determined whether existing information systems will be able to process anticipated transaction increases associated with the Recovery Act. There was a lack of coordination between Headquarters organizations related to aspects of Recovery Act reporting. The need to report accurate and complete information to the public and the Office of Management and Budget (OMB) is a Recovery Act imperative. In addition, we are concerned that the Department's information systems supporting Recovery Act activities may be unable to handle significant increases in workload or provide appropriate mechanisms to ensure that funds are accurately tracked and reported.

- Special Report on *The American Recovery and Reinvestment Act at the Department of Energy* (OAS-RA-09-01, March 2009). The report identified specific risks that were discovered during past reviews and investigations in areas such as fund accounting and reporting, grants and cooperative agreements, contract management, and loan guarantees. While the use of grants and cooperative agreements can be an effective way to fund various initiatives, these types of financial assistance tools also carry a number of demonstrated risks. Our prior reviews have also established that program officials did not always take action to mitigate performance-related risks through effective monitoring of grants and cooperative agreements. To prepare for the vast increase in projects funded through grants and cooperative agreements, and to address the risks we have previously identified, the Department should take steps to: develop aggressive safeguards to ensure

that financial and business risks are adequately assessed and addressed prior to initial award; monitor performance throughout the life-cycle of the grant or cooperative agreement; and adjust project management techniques to ensure the transparency of project data and ensure that specific OMB and Recovery Act monitoring and reporting requirements are met. Controls such as these are essential to ensuring that the massive surge in funds to be distributed through grants and cooperative agreements is adequately controlled and monitored. Based on current plans, these funding mechanisms are to form a significant part of Recovery Act outlays and are therefore likely to be critical to achieving desired economic stimulus.

- *Management of the Department's Publicly Accessible Websites* (DOE/IG-0789, March 2008). The audit identified several opportunities to improve the security and management of the Department's publicly accessible websites. Specifically, we identified numerous significant cyber security incidents, which, in our judgment, could have been prevented had proper security controls been in place; content on publicly accessible web servers was not always controlled and reviewed periodically; and most of the organizations reviewed also had not incorporated contingency/emergency planning features, provided accessibility for individuals with disabilities, and/or disabled unneeded computer services for their publicly accessible websites. We concluded that the risk that the Department's publicly accessible websites and the data they contained could be compromised was higher than acceptable. A lack of guidance from Headquarters and deficiencies in site-level management and control contributed to an unnecessarily risky security posture and publicly accessible websites that did not meet Federal accessibility requirements or contingency planning and emergency response best practices.

Department of Energy
Washington, DC 20585

JUL 06 2010

MEMORANDUM FOR: RICKEY R. HASS
DEPUTY INSPECTOR GENERAL FOR
AUDIT SERVICES
OFFICE OF INSPECTOR GENERAL

FROM: KATHLEEN B. HOGAN
DEPUTY ASSISTANT SECRETARY
FOR ENERGY EFFICIENCY
OFFICE OF TECHNOLOGY DEVELOPMENT
ENERGY EFFICIENCY AND RENEWABLE ENERGY

SUBJECT: Response to the Office of Inspector General Draft Report on the Audit 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"

The U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy (EERE) appreciates the opportunity to review and comment on the results of the Audit performed on the Management Controls over the Department's Performance and Accountability for Grants in Energy (PAGE) system for Energy Grants Management under the American Recovery and Reinvestment Act (ARRA or Recovery Act).

Recommendation 1: A risk-based approach is taken when developing and implementing information systems, including review of development and implementation efforts at the appropriate management level.

Response: EERE concurs in part with the recommendation.

Management Response: EERE recognizes the importance of a risk-based approach when developing and implementing information systems. While seeking to mitigate risk, EERE also found it necessary to accommodate compressed timelines imposed by the Recovery Act, and ensure cost-effectiveness in conducting system security activities on PAGE.

EERE explored multiple options for conducting certification and accreditation activities. The approach that was applied was deemed appropriate for a system that was undergoing phased development and a relatively high pace of change. PAGE development was divided into four phases and EERE believes it was able to achieve a cost-balanced and risk-based approach by performing all the required steps of a certification and accreditation after major phases of system development (specifically, after Phase One and Phase Three).[1] An initial risk assessment was

[1] EERE followed National Institutes of Standards and Technology (NIST) Guidance as outlined in Special Publication 800-30, Risk Management Guide for Information Technology Systems, which states that "Organizations may choose to expand or abbreviate the comprehensive process and steps suggested in this guide and tailor them to their environment in managing IT-related mission risks."

conducted during early development, and the weaknesses were identified and documented in the initial Plan of Action and Milestones (POA&M) following Phase One. Prior to beginning Phase Two, EERE developed initial versions of the System Security Categorization, System Security Plan, Security Assessment Report, and Privacy Impact Assessment.

Action Plan: Following Phase Three of development, an independent security test and evaluation will be conducted, during which remaining weaknesses will be identified, prioritized, and corrected as documented in the POA&M.

Estimated Date of Completion: September 30, 2010

Recommendation 2: Appropriate security protection measures over the PAGE system are implemented and tested using a risk-based approach in the most expeditious manner possible.

Response: EERE concurs with the recommendation as stated.

Management Response: PAGE is undergoing a full Security Test and Evaluation (ST&E) Review, which began the week of June 21, 2010. The ST&E will determine the system's compliance with defined security requirements by testing the correctness and effectiveness of the security controls related to:

- Hardware, software, operating system, applications, and databases
- Increased levels of concern for confidentiality, integrity, and availability, and
- Internal or external exposure, and risk-based decisions

The ST&E documents effective security controls and identifies security controls that are either ineffective or insufficiently implemented. The latter are documented in a Risk Assessment intended to define the residual risk prior to mitigation, and after appropriate risk mitigation has occurred.

Estimated Completion Date: September 30, 2010

Recommendation 3: Effective project management practices are implemented as part of ongoing and future development efforts for information technology systems, to include evaluation of viable alternatives, completion of detailed cost and alternatives analyses, acquisition planning, and market research prior to making funding decisions.

Response: EERE concurs in part with the recommendation.

Management Response: EERE recognizes the need for effective management practices as part of ongoing and future information technology development efforts. EERE will ensure compliance with OMB Project Management Practices, and alternatives analysis for IT investments will be completed in advance of project implementation.

With regard to the PAGE system, in December 2008, EERE completed an interim report that contained several alternatives which were considered for a web-based solution. While the final report was not formally issued until June 2009, the critical components identified in February 2009 provided EERE with the necessary information to initiate the development efforts required to meet the timeframes established by Recovery Act.

Action Plan: EERE has developed an action plan to conduct an alternatives analysis related to future PAGE development efforts, including review of requirements, detailed costs, and market research. This analysis is being conducted in conjunction with the Office of the Chief Information Officer (OCIO) as part of EERE's ongoing implementation of effective project management practices.

Estimated Completion Date: September 30, 2010

Attachments

IG Report No. OAS-RA-10-14

CUSTOMER RESPONSE FORM

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

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

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

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

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

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

Name _____ Date _____

Telephone _____ Organization _____

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

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

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Felicia Jones 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://www.ig.energy.gov

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