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

Audit Report

Management Controls over the Department's WinSAGA System for Energy Grants Management Under the Recovery Act

OAS-RA-10-05

March 2010

Department of Energy
Washington, DC 20585

March 25, 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 Department's WinSAGA System for Energy Grants Management Under the Recovery Act"

BACKGROUND

As a result of the American Recovery and Reinvestment Act of 2009 (Recovery Act), the Department of Energy (Department) received $8.1 billion for formula grant programs supporting housing weatherization and energy efficiency. This amount is significantly larger than the approximately $300 million historically received each year for such purposes. To help control performance, the Department established an incremental approach to awarding funding to states, releasing funds based on performance. To aid in making incremental funding decisions, the Department intends to track recipients' performance through the Windows System Approach to Grants Administration (WinSAGA). WinSAGA, a custom-designed information system, is utilized by the Department and more than 70 state-level program offices to collect, organize, distribute, and report a wide array of information relating to the energy formula grant programs. According to WinSAGA security documentation, the system and the information it houses requires enhanced protection measures to help ensure, among other things, that confidentiality is properly maintained.

WinSAGA is now being utilized by the Department to manage grants and fulfill certain Recovery Act reporting requirements. In addition, WinSAGA is used by state-level program offices and the Department to apply for and manage the grants awarded under the Recovery Act for the State Energy and Weatherization Assistance Programs. Because of WinSAGA's role in reporting on and managing Recovery Act related awards, we initiated this audit to determine whether current system resources and controls were adequate.

RESULTS OF AUDIT

In general, WinSAGA, as currently configured, appeared to be capable of processing the additional formula grant transactions resulting from the Recovery Act. We did, however, identify certain security concerns with the system that 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. These practices were contrary to Federal and/or Departmental requirements and could have allowed unauthorized changes to be made to grant data;

- 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; and,

- Security planning documentation and control testing were incomplete and contained several inconsistencies. For example, the information contained in the system security plan was not representative of the entire computing environment and testing of the system excluded a significant portion of required security controls.

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. In particular, we noted that responsibility for communicating cyber security requirements to system administrators and users had either not been assigned or had not been met. In addition, the approach used to ensure that corrective actions adequately addressed security weaknesses was not always effective. While we found no evidence of compromise, 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.

In an effort to meet increasing security requirements, a web-based replacement system, Performance and Accountability for Grants in Energy (PAGE), is under development. This system will completely replace WinSAGA and was planned for initial implementation in June 2009 with functionality for the State Energy and Weatherization Assistance Programs maintained in WinSAGA being available by December 2009. At that time, it was expected that WinSAGA would be decommissioned. Officials recently announced, however, that it is likely this functionality will not be available in PAGE until at least the middle of Fiscal Year 2010. The Office of Energy Efficiency and Renewable Energy noted that PAGE will utilize many of the same managerial controls as WinSAGA and be managed by the same contractor. The new system will incorporate all existing WinSAGA data and will also be used to manage additional grants made available through the $3.2 billion Recovery Act Energy Efficiency and Conservation Block Grant program. In light of the uncertainty surrounding the timing of the transition to PAGE and the importance of the data currently maintained in WinSAGA, action is needed to address existing system weaknesses. Further, management needs to ensure that the same or similar issues do not develop during the design and transition to PAGE. To address these issues, we have made several recommendations which, if fully implemented, should help improve the security posture of the energy grant management systems.

MANAGEMENT REACTION

Management generally concurred with the recommendations and indicated that steps were being taken to address many of the issues identified in our report. Management also commented that it will work to ensure that the weaknesses noted in our report are addressed as part of the implementation of PAGE. Management's comments are included in their entirety 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 DEPARTMENT'S WINSAGA SYSTEM FOR ENERGY GRANTS MANAGEMENT UNDER THE RECOVERY ACT

TABLE OF CONTENTS

Energy Grant Management System Controls

Appendices

Management Controls over the Department's WinSAGA System for Energy Grants Management Under the Recovery Act

Energy Grant Management System Controls

We found that, as currently configured, the Windows System Approach to Grants Administration (WinSAGA) system appeared to possess sufficient capacity for processing additional formula grant transactions resulting from the American Recovery and Reinvestment Act of 2009 (Recovery Act). However, we identified a number of instances where system security controls may not be completely effective. Specifically, we noted certain weaknesses related to system access, system backup and recovery, and security documentation and control testing that could adversely affect the overall reliability, confidentiality, and availability of the system and the information it maintained.

Office of Energy Efficiency and Renewable Energy (EERE) officials assessed WinSAGA as a moderate impact system in accordance with Federal guidelines where the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, assets, or individuals. Program officials indicated that its replacement system – Performance and Accountability for Grants in Energy (PAGE) – is anticipated to have the same risk level and would contain security controls similar to WinSAGA. Therefore, if the issues identified in our report are not adequately considered and fully addressed, PAGE may also not have the protection measures necessary to ensure overall reliability, confidentiality, and availability of the system and the information that it will maintain.

System Access

We identified weaknesses in a number of access control areas for WinSAGA. Access controls consist of both physical and logical measures designed to protect information resources from unauthorized modification, loss, or disclosure. Proper implementation of such controls is necessary to reduce the overall risk to the system. We found, however, that:

- Although the National Institute of Standards and Technology (NIST) required that users be given the lowest level of access to the system that is required to perform their duties, user access privileges were not always consistently assigned and based on user need. Specifically, we found that more than 40 of 70 state-level program offices reviewed granted the highest level of available access privileges. Within these offices, we

determined that almost half of the active users had been assigned such privileges to the system's primary modules. In contrast, 20 of the 70 state-level program offices did not assign this level of access to any users. Furthermore, this practice was contrary to the WinSAGA system security plan which directed that users be provided system access based on the principle of "least privilege." Granting users privileges in excess of those needed could allow unauthorized modifications to system information and permit users to modify performance data – actions that could ultimately impact funding decisions. Since WinSAGA does not log such modifications, officials would likely not be able to identify the source of unauthorized modifications. In response to our draft report, management stated that it had initiated action to review and adjust system user accounts to ensure that all users' access levels were limited to those needed to perform their job duties.

- The password change configuration process for WinSAGA was insufficient for a moderate risk system. In particular, although the Energy Program Cyber Security Plan (PCSP) required user account passwords to be changed at least every six months, the WinSAGA system security plan only required passwords to be changed after 500 logins. Based on this information, we estimated that a user would have needed to log into the system an average of four times a day to reach the 500 login threshold within a six month period. If a user had logged into the system just once a day, it would have taken almost two years to meet the program requirement for a password change. Three users we spoke with disclosed that they had never changed their passwords. When passwords are not regularly changed, the risk of an undetected system compromise through the use of various techniques to obtain and/or guess users' passwords increases substantially. Management indicated in its comments to our report that, as a result of our review, it had implemented a process that required passwords to be reset after 183 days.

- A previously identified weakness related to password complexity had not been fully resolved. Specifically, in 2007, EERE management directed that a configuration change be made to enforce complexity requirements for passwords associated with WinSAGA user accounts.

This change was made to the Headquarters' servers via settings within the operating system and reported as corrected or closed in the system's Plan of Action and Milestones (POA&M), a tool used by management to track and monitor the progress of cyber security corrective actions. However, the change for enforcing authentication requirements through the application was not validated on servers at the state level, thus leaving the state-level servers – computers that contain the vast majority of the WinSAGA system infrastructure – potentially vulnerable to compromise. Program officials noted that they had taken action to resolve this issue after our fieldwork was completed.

System Backup and Recovery

Contrary to Federal and Department of Energy (Department) requirements, appropriate system backup and recovery procedures had not been implemented for WinSAGA. NIST and Department directives require that information backups for moderate risk systems be properly secured and stored in a location that is geographically separate from the primary processing facility. Although the backups should have been moved from the system and secured in a timely manner, we noted that the files were retained on the system for an extended period before being moved to a portable device and stored at the system administrator's residence. This weakness was identified at the time of security testing and certification of the system for operation in July 2007. However, even though system officials had committed to correcting the deficiency at that time, our review identified that it had not been resolved. In response to our draft report, management stated that alternative storage arrangements had been made to ensure that system backups were properly secured.

In addition, annual testing of WinSAGA's contingency plan did not ensure the timely recovery of information and system operations in the case of service disruption. Contrary to requirements in the Energy PCSP, the contingency plan and the methodology utilized in the plan testing for Fiscal Year 2008 disclosed that a live recovery was not performed. Furthermore, the scope of the testing performed was limited to the main application servers at Headquarters, excluded testing of other servers that were part of the system, and involved a scenario not requiring plan activation. In addition, eight weaknesses identified as a result of testing in July 2008 were not included

in the POA&M to ensure that they could be effectively tracked and resolved. Even though management commented that these items had been closed in the POA&M, we noted that the weaknesses still had not been fully addressed at the time of our review.

Security Documentation and Testing

Security planning documentation and control testing for WinSAGA was incomplete and contained several inconsistencies. For example, the system security plan was not representative of the entire computing environment – only including the main Headquarters servers and excluding the servers used by the 70 state-level program offices. Therefore, security control testing designed to support management's decision to authorize the system to operate and accept the risk of such operation was only conducted on the servers located at Headquarters. Testing was not performed on the state-level servers to ensure that the required controls were in place and operating as expected. EERE officials stated that the decision to limit the scope of testing on the WinSAGA system was initially made in 2004 because the system was scheduled to be decommissioned. However, this did not occur and the limitation was carried forward when the system was tested again in 2007. By limiting the scope of testing on the system, EERE essentially reduced the system's boundary and could not sufficiently attest to the security of the state level servers. Had testing on the state level servers been completed, security vulnerabilities such as weak passwords could have been identified and remediated.

Our analysis of the System Security Plan found that it excluded 16 percent of the security controls and control enhancements that were required by NIST for a moderate risk system. For example, several controls related to the areas of system access, audit and accountability, and system and communications protection had not been addressed. Furthermore, where testing was completed on the Headquarters level servers, almost ten percent of the control test results were inconsistent with the results reported in the system security plan. For example, we identified 13 controls for which testing results had been documented in the Security Assessment Report as being implemented even though the System Security Plan indicated – sometimes erroneously – that these controls were not applicable to the WinSAGA environment.

Communication and Performance Monitoring

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. In particular, we noted that specific responsibility for communicating cyber security requirements to system administrators and users had not been assigned for the system by EERE. In addition, the method and approach used to validate corrective actions taken to close POA&M items was not always effective.

Communication of Security Requirements

EERE officials had not ensured that responsibility was assigned for communicating all cyber security requirements to the Information System Security Officer (ISSO) – the individual responsible for ensuring security of the information system – and system users. Specifically, the EERE Cyber Security Program Manager was the only official assigned responsibility for security over the program's systems. However, the Energy PCSP disclosed that the responsibilities of this position focus on the overall management of the cyber security program rather than ensuring that requirements are implemented on specific systems. Our review found that no one within EERE had been assigned the responsibility of ensuring that system specific requirements were properly communicated to the system ISSO. Thus, although NIST required that system accounts be reviewed at least annually to determine whether they remain valid, officials had not ensured that periodic access reviews were completed so that users who no longer had a valid need to access the system were denied access to the system. We also found that WinSAGA's audit event logs were not periodically reviewed for inappropriate or unusual activity as required by NIST. Further, because system-level responsibility had not been assigned by the program, weaknesses related to contingency planning identified after the system was authorized to operate were not recorded in the POA&M as noted previously in our report.

The WinSAGA ISSO also had not ensured that the system's security requirements were fully communicated to all users. Even though the system's security documentation contained requirements with which all users were expected to comply, officials from all seven state-level offices contacted disclosed that the system security requirements had not been shared with

them. They also indicated that they had not been contacted at any time regarding security control implementation, such as password complexity, user access, and audit log review.

Plan of Action and Milestones Validation

We also noted that the method and approach used to validate corrective actions taken to close POA&M items was not always effective. During our review, we observed that security weaknesses existed even though the program reported them as corrected and closed. For instance, although reported as being fully remediated prior to our audit, corrective actions related to password configuration complexity weaknesses were not taken until we brought the issue to management's attention during our review. In addition, a weakness related to the appropriate storage of backups for WinSAGA still existed at the time of our review. These issues are similar to those noted in our evaluation report on *The Department's Unclassified Cyber Security Program – 2008* (DOE/IG-0801, September 2008), which identified weaknesses throughout the Department related to the utilization of POA&Ms for tracking and correcting all known cyber security weaknesses. In response to our recommendation, EERE management reported that it properly utilized the POA&M to track the remediation of identified cyber security issues. However, based on our review, we noted that additional improvements are needed in the EERE POA&M process.

Risk to Systems and Sensitive Information

Without improvements, WinSAGA, and the information it maintains, may be exposed to a higher than necessary level of risk of compromise, loss, modification, and non-availability. For instance, system access weaknesses could be exploited to either favorably or unfavorably modify performance results. Because Recovery Act funds for the State Energy and Weatherization Assistance Programs are being awarded in increments, such modifications could impact future funding decisions. Since future award decisions will be made based on the states' performance with currently awarded funds, the data within WinSAGA and its successor system, PAGE, must be reliable to ensure that decisions related to the timing and amount of future awards are not based on flawed data. Furthermore, inadequate system recovery procedures could impact the availability of data at key mission-related decision points. For instance, weak backup and recovery procedures

could result in the loss of data which may significantly impact EERE's and the states' ability to meet quarterly reporting requirements under the Recovery Act.

As previously noted, WinSAGA is scheduled to be replaced by PAGE. Because both systems have been identified as moderate impact systems, EERE officials noted that PAGE is expected to have a similar control structure to that of WinSAGA. While program officials stated that there was a lack of reportable security incidents or unscheduled outages involving WinSAGA, we noted that the WinSAGA system had limited network connectivity and, as such, was isolated from many types of external attacks. However, its replacement system, PAGE, will be accessed over the Internet and, therefore, will inherently encounter more security vulnerabilities and threats.

As a result, the continuation of current practices, especially those noted in our report, could be detrimental to the management of the state-level energy formula grant programs, as well as the Energy Efficiency and Conservation Block Grant program involving local municipalities, both of which will utilize PAGE. In addition, because PAGE will be a custom-built web-based application that is accessed over the Internet, properly securing it takes on a greater level of importance. As previously reported in our report on *Management of the Department's Publicly Accessible Websites* (DOE/IG-0789, March 2008), web-based applications were cited by industry experts as being particularly vulnerable to exploit. Furthermore, industry experts recently reported that 60 percent of successful Internet attacks were launched against web applications, the vast majority of which were custom built. Absent corrective action, it may be difficult to ensure that PAGE is adequately protected. In responding to our draft report, program officials stated that they would address issues identified with WinSAGA and take action to ensure that similar weaknesses are addressed during the development of PAGE.

RECOMMENDATIONS

To improve the effective and secure management of the Department's energy grant management applications, we recommend that the Assistant Secretary for Energy Efficiency and Renewable Energy ensure that:

1. Responsibility is assigned to an appropriate individual to ensure that cyber security policies and practices are

properly communicated to the ISSO and state-level program offices in accordance with Federal and Department requirements for WinSAGA and its successor system, PAGE;

2. Corrective actions taken to address security weaknesses are appropriately tracked and validated prior to closing POA&M items; and,

3. Existing weaknesses in WinSAGA are resolved to the extent practical and appropriate based on the system's anticipated retirement date.

MANAGEMENT REACTION

Management generally concurred with the recommendations and indicated that steps were being taken to address many of the issues identified in the report. However, management expressed concerns with several of the assertions made in our report. We have addressed management's concerns below and made technical changes to the report, as appropriate. Management's comments are included in their entirety in Appendix 3.

Management disclosed that the EERE Cyber Security Program Manager lacked sufficient staffing to ensure separation of duties with the Cyber Security Program. However, management believed that the limited scale of the Cyber Security Program allowed it to operate without the recommended segregation of duties and principle of least privilege implemented. In addition, management indicated that it would design and implement a new POA&M management process for all Headquarters systems, including WinSAGA and PAGE. Furthermore, management commented that it had made the decision to limit the scope of the certification and accreditation process and focus on critical cyber security updates, noting that WinSAGA will be decommissioned in June 2010 and proper security controls will be implemented on the PAGE system.

Management commented that annual contingency plan testing was conducted in accordance with the Under Secretary of Energy PCSP. According to management, this document permitted moderate level systems to undergo testing using tabletop exercises. To that end, management stated that it would continue to utilize tabletop testing on both the WinSAGA and PAGE systems.

Management commented that security control testing was limited to only the Headquarters servers to allow a manageable scope for the effort. Specifically, the decision was made in 2004 not to include the 70 state-level offices in testing due to limited resources and the expectation that the system would be replaced in the near future. Management noted that PAGE will have a less distributed architecture and testing for that system will encompass all components of the system.

Furthermore, management disclosed that the most recent system certification, which took place in 2007, was conducted prior to the issuance of the initial version of the Under Secretary of Energy PCSP. Therefore, many of the requirements currently addressed within that document are not covered by the WinSAGA security plan. In addition, management indicated that some of the security controls we noted as being excluded in our report were identified as 'Not Applicable' in the system security plan.

AUDITORS COMMENTS

Management's comments are responsive to our recommendations. However, we continue to believe that issues related to system backup and recovery, as well as security control documentation and testing, remain valid concerns. Furthermore, we agree that WinSAGA will be decommissioned and that major modifications to the system at this time may not be value-added. However, we continue to urge management to ensure that these areas are fully addressed as part of PAGE development and implementation. Management's response to our report disclosed that many of the issues identified with WinSAGA would be addressed in PAGE. We will review management's actions as they relate to PAGE as part of an ongoing review.

In response to management's comment regarding the required level of annual contingency plan testing, we noted, and Department officials confirmed, that the Energy PCSP required moderate systems to undergo functional exercises that are more extensive than tabletop testing and directed that an event that would require activation of the contingency plan be simulated.

We also noted that management's decision to limit the scope of system certification testing reduced the security boundary of the system to encompass only the Headquarters aspect of the system. In this case, we would have expected that this limitation be documented in the system security plan and

addressed as a residual risk to be considered by the Designated Approving Authority when granting the system authority to operate.

We agree that the Energy PSCP had not been issued at the time the WinSAGA system security plan was updated in 2007. In this case, EERE should have documented and implemented the controls required by NIST Special Publication 800-53 for a moderate system. Our comparison of NIST guidance with the system security plan verified that there were 34 controls or control enhancements that were not addressed – accounting for 16 percent of the required controls and enhancements. Although we found that several controls documented in the security plan were labeled as being not applicable to the WinSAGA environment, those controls were not included in the calculations noted in our report.

Appendix 1

OBJECTIVE

To determine whether current system resources were adequate to handle the increased activity resulting from the American Recovery and Reinvestment Act of 2009 (Recovery Act), and whether the necessary controls for ensuring the accuracy, integrity, and completeness of information had been implemented and were operating as intended.

SCOPE

The audit was performed between May 2009 and January 2010 at Department of Energy (Department) Headquarters in Washington, DC.

METHODOLOGY

To accomplish the audit objective, we:

- Reviewed applicable laws and Department directives, including those pertaining to grants management under the Recovery Act;
- Reviewed applicable standards and guidance issued by the Office of Management and Budget related to accounting and reporting requirements of the Recovery Act;
- 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 and contractor personnel relating to system security and controls, and system capability, changes, and use for Recovery Act purposes; and,
- Analyzed documentation to determine whether selected system controls were in place and operating as intended.

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 the Office of Energy Efficiency and Renewable Energy'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 not rely on computer-processed data to satisfy our objectives.

An exit conference was held with Department officials on March 25, 2010.

RELATED REPORTS

- Audit Report on *"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). We found that 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. We did, however, identify certain issues relating to American Recovery and Reinvestment Act of 2009 (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 and 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. 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.

- Audit Report on *"Protection of the Department of Energy's Unclassified Sensitive Electronic Information"* (DOE/IG-0818, August 2009). Our review identified opportunities to strengthen the protection of all types of sensitive unclassified electronic information and reduce the risk that such data could fall into the hands of individuals with malicious intent. In particular, sites had either not ensured that sensitive information maintained on mobile devices was encrypted or they had improperly permitted sensitive unclassified information to be transmitted unencrypted through email or to offsite backup storage facilities; had not ensured that laptops taken on foreign travel were protected against security threats; and were still working to complete Privacy Impact Assessments. Our testing revealed that the weaknesses identified were attributable, at least in part, to Headquarters programs and field sites that had not implemented existing policies and procedures requiring protection of sensitive electronic information. As demonstrated by previous computer intrusion-related data losses throughout the Department, without improvements, the risk or vulnerability for future losses remains unacceptably high.

- 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 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.

- Evaluation Report on *"The Department's Unclassified Cyber Security Program - 2008"* (DOE/IG-0801, September 2008). We found that while the Department continues to make incremental improvements in its unclassified cyber security program, certain problems persisted such as issues with system certification and accreditation and contingency planning. These internal control weaknesses existed, at least in part, because not all Department program organizations, including the National Nuclear Security Administration, had revised and implemented policies incorporating Federal and Departmental cyber security requirements in a timely manner. Program officials had also not effectively performed management review activities essential for evaluating the adequacy of cyber security performance. Consequently, the risk of compromise to the Department's information systems remained higher than necessary with additional action needed to reduce this risk.

- Audit Report on *"Management of the Department's Publicly Accessible Websites"* (DOE/IG-0789, March 2008). Our 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.

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

FROM: KATHLEEN B. HOGAN(NO SIGNATURE-508 VERSION)
DEPUTY ASSISTANT SECRETARY
FOR ENERGY EFFICIENCY
OFFICE OF TECHNOLOGY DEVELOPMENT
ENERGY EFFICIENCY AND RENEWABLE ENERGY

SUBJECT: Comments to the Office of Inspector General Draft Report on the Audit of "Management Controls over the Department's WinSAGA System for Energy Grants Management Under the Recovery Act"

The Department of Energy (DOE) 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 WinSAGA System for Energy Grants Management under the Recovery Act. WinSAGA is a system that has been in production since January 1999 with zero (0) identified or reported incidents of data compromise and no significant events of unscheduled system unavailability. As noted in the report, WinSAGA is scheduled to be retired in June 2010. The report indicates that the WinSAGA functionality was initially planned for a June 2009 implementation in PAGE; however, the WinSAGA functionality to be migrated over to PAGE was originally scheduled for a December 2009 implementation. In June 2010, EERE is planning on decommissioning the WinSAGA system, which will be replaced by the Performance and Accountability for Grants in Energy (PAGE) system. The PAGE system is a web-based system with similar functionality and data as WinSAGA. PAGE and WinSAGA have some overlaps when it comes to the managerial controls, notably the personnel managing the system and certain policies and procedures; however, the technical architecture of this system is entirely different from WinSAGA. The PAGE system has been built to be in compliance with Department of Energy regulatory guidance, while also ensuring that the weaknesses noted within the Draft Report on the Audit of "Management Controls over the Department's WinSAGA System for Energy Grants Management Under the Recovery Act" are proactively addressed so that the system will be in compliance with all prescribed Federal and Departmental directives.

The Audit contains three (3) recommendations that its authors believe are necessary to ensure the effective and secure management of the Department's energy grant management applications.

First, the Audit recommends that "Responsibility [be] assigned to an appropriate individual to ensure that cyber security policies and practices are properly communicated to the ISSO [Information System Security Officer] and state-level program officers in accordance with Federal and Departmental requirements for WinSAGA and its successor system, PAGE." In response, we note that, due to a lack of resources, the EERE Cyber Security Program Manager lacks sufficient staffing to ensure separation of duties within the Cyber Security Program (CSP). While not ideal, the limited scale of the Cyber Security Program allows it to operate without the recommended segregation of duties and the principle of least privilege implemented. Additionally, although the report states that access reviews are not performed

regularly and inactive accounts are not deleted, internal IV&V testing verified that all users from all user groups (HQ, PMC, and states) that have not logged in to the WinSAGA application within 183 days, will be prevented from accessing the application. For the PAGE system, EERE will look to establish greater depth of resources within the Cyber Security Program so that the EERE Cyber Security Program Manager is not the only official assigned responsibility for security over the program's systems. This will allow the CSP to meet both organizational changes and pending growth challenges improving program efficiency, overall communication between program stakeholders, and general collaboration.

Second, the Audit recommends that "Corrective actions taken to address security weaknesses [be] appropriately tracked and validated prior to closing POA&M (Plan of Action and Milestones) items." In response, we note that, as a result of IG's suggestion, EERE will be designing and implementing a new POA&M Milestone/Weakness Verification process for all Headquarters systems, including WinSAGA and PAGE. EERE will have an independent verifier, review and physically verify the corrective action taken for each milestone and weakness for all Headquarter systems, prior to them being updated as "Verified" within the POA&M. This will ensure that no WinSAGA or PAGE POA&M items are closed as remediated and in place without the corrective action actually being thoroughly performed on each respective system.

Finally, the Audit recommends that "Existing weaknesses in WinSAGA [be] resolved to the extent practical and appropriate bases on the system's anticipated retirement date." In response, we note that WinSAGA's distributed architecture has been a concern for the past several years. Due to a lack of resources for conducting testing at the 70+ state offices and since WinSAGA has been scheduled for decommissioning for a number of years, EERE has made the decision to limit the scope of the Certification &Accreditation (C&A) process and other systems improvement processes, and to not allow their scope to expand beyond a manageable effort for a system with a limited life expectancy. Instead, the WinSAGA support team has focused on critical updates, for instance by reducing the number of WinSAGA users by removing inactive accounts along with decreasing the access rights of various users who were deemed to not be in compliance with the principle of least privilege. WinSAGA is set to be decommissioned in June 2010 and proper security controls will be implemented on the PAGE system.

The PAGE system is a web-based system that will not have a distributed environment with servers across the country. Therefore, the PAGE C&A and respective System Security Plan encompasses all components of the system and accreditation boundary.

Our specific comments on your findings are given in the attachment.

Attachment

Department of Energy Response to Office of Inspector General Draft Audit Report
on
Management Controls over the Department's WinSAGA System for Energy Grants Management Under the Recovery Act

OIG FINDINGS

System Access	
Finding #1	The draft report states that "….more than 40 of 70 state-level program offices reviewed granted the highest level of available access privileges. Within these offices, we determined that almost half of the active users had been assigned such privileges to the system's primary modules."
Management's Response	Concur
Departmental Response	When the WinSAGA support team was informed of this initial draft in late November 2009, they proactively began a review of WinSAGA user access levels for sites where all users had full access to the grant and state application modules. The WinSAGA support team reduced the number of WinSAGA users by removing inactive accounts along with decreasing the access rights of various users who were deemed to not be in compliance with the principle of least privilege. In addition to user access levels, there are WinSAGA edits based on business rules that prevent users from updating or deleting information under pre-defined conditions. Moreover, WinSAGA record ownership prevents any changes from being made by a State office to data when DOE has ownership. Moving forward for the PAGE system, Grantee users will be required to acknowledge acceptance of the PAGE Rules of Behavior document, which discusses the principle of least privilege. Additionally, the Local System Administrator for each grant will be provided Access Control Management procedures which provide explicit instructions for account creation to ensure that specific roles are segregated to ensure the principle of least privilege. Lastly, the PAGE support team is currently evaluating application-level configuration changes to limit local system administrator accounts.
Finding #2	The draft report states that "The password change configuration process for WinSAGA was insufficient for a moderate risk system. In particular, although the Energy Program Cyber Security Plan (PCSP) required user account passwords to be changed at least every six months, the WinSAGA system security plan only required passwords to be changed after 500 logins."
Management's Response	Concur
Departmental Response	The WinSAGA application forces a password reset after 183 days. The PAGE application will force all users to change their passwords after 180 days, which is equivalent to six (6) months and in compliance with the minimum requirements stated in the

	governing policy, the DOE Under Secretary of Energy Program Cyber Security Plan (PCSP) v 1.2.
Finding #3	The draft report states that "….Specifically, in 2007, EERE management directed that a configuration change be made to enforce complexity requirements for passwords associated with WinSAGA user accounts. This change was made to the Headquarters' servers via settings within the operating systems…..however; the change for enforcing authentication requirements through the application was not validated on the servers at the state level."
Management's Response	Concur
Departmental Response	The WinSAGA support team verified that State users are required to have a password with a least 8 characters, with a combination of letters and numbers, and at least one special character. EERE acknowledges that password complexity requirements should be enforced consistently across all WinSAGA platforms, including DOE and states. PAGE is a web-based application with centralized password management. The PAGE application's password complexity is in compliance with the DOE Under Secretary of Energy PCSP v 1.2, PWM-50, page 89, as follows: (a) Passwords contain at least eight non-blank characters. (b) Passwords contain a combination of letters, numbers, and at least one special character within the first seven positions. (c) Passwords contain a nonnumeric in the first and last position. (d) Passwords do not contain the user ID. (e) Passwords do not contain any common English dictionary word, spelled forward or backwards (except words of three or fewer characters). (f) Passwords do not employ common names. (g) Passwords do not contain commonly used numbers associated with the user of the password. (h) Passwords do not contain any simple pattern of letters or numbers.

System Backup and Recovery	
Finding #4	The draft report states that, "….appropriate system backup and recovery procedures had not been implemented for WinSAGA…..Although the backups should have been moved from the system and secured in a timely manner, we noted that the files were retained on the system for an extended period before being moved to a portable device and stored at the system administrator's residence."

Management's Response	Concur
Departmental Response	WinSAGA differential backups are performed nightly with a full backup performed on a weekly basis. On a weekly basis, backups are rotated off-site to a bank vault at the SunTrust Bank in Gaithersburg, MD. Therefore, backups are moved from the system and secured in a timely manner. For the PAGE system, system level and data backups will be conducted on a daily basis by the EERE IT Department. Full back-ups will be performed every weekend and differential back-ups will be performed nightly. Backup tapes will be secured in a locked cabinet while onsite at Forrestal. Access to the locked cabinet is limited to system administrators. EERE also has an arrangement with Iron Mountain for offsite storage of backup tapes in Richmond, VA, which is approximately 100 miles from the production location. Additionally, EERE is currently developing a plan for an alternate processing site at NETL. When finalized, production data will be replicated to the Disaster Recovery Servers located in Morgantown, WV in real-time.
Finding #5	The draft report states that, "In addition, annual testing of WinSAGA's contingency plan did not ensure the timely recovery of information and system operations in the case of service disruption. Contrary to program-level direction, the contingency plan and the methodology utilized in the plan testing for Fiscal Year 2008 disclosed that a live recovery was not performed."
Management's Response	Non-Concur
Departmental Response	Per the 2007 WinSAGA Certification & Accreditation (C&A), the system was rated as a "Moderate" system. Per the DOE Under Secretary of Energy Program Cyber Security Plan (PCSP) v 1.2, moderate systems are only required to perform a Tabletop Exercise on an annual basis for the testing of their respective Information Technology Contingency Plans (ITCPs). Additionally, during the ITCP testing it was noted that the exact process that would be followed to reconstitute WinSAGA in the event of a disaster at Headquarters would be performed from a different location if the system were to go down at one of the state sites. The PAGE ITCP will perform a tabletop exercise on an annual basis, per the requirements outlined in the DOE Under Secretary of Energy PCSP v 1.2.
Finding #6	The draft report states that, "….In addition, eight weaknesses identified as a result of testing in July 2008 were not included in the POA&M to ensure that they could be effectively tracked and resolved."
Management's Response	Concur
Departmental Response	The eight (8) weaknesses identified during the WinSAGA testing in July 2008 had been previously put on a POA&M and were closed. However, these items mistakenly showed up on the WinSAGA

	ITCP Testing – After Action Report and were mistakenly never removed from the report. Therefore, it was noted by the OIG that weaknesses noted during ITCP testing were never included onto a POA&M for tracking purposes. Moving forward, all contingency plans testing for WinSAGA will include an After-Action report where all weaknesses and areas of non-compliance identified are to be immediately placed on a POA&M to ensure they can be effectively tracked and resolved. For the PAGE system, ITCP testing will be conducted on an annual basis. Upon completion of the ITCP testing an After-Action report will be generated documenting all weaknesses and areas of non-compliance. Lastly, all weaknesses and areas of non-compliance identified are to be immediately placed on a POA&M to ensure they can be effectively tracked and resolved.

Security Documentation and Testing	
Finding #7	The draft report states that, "Security planning documentation and control testing for WinSAGA was incomplete and contained several inconsistencies. For example, the system security plan was not representative of the entire computing environment – only including the main Headquarters servers and excluding the servers used by the 70 state-level program offices"
Management's Response	Concur
Departmental Response	WinSAGA's distributed architecture has been a concern for the past several years and a decision was made in order to have a manageable project scope for the initial C&A effort in 2004. Due to a lack of resources for conducting testing at the 70+ state offices and since WinSAGA has been scheduled to be decommissioned for a number of years the decision was made to limit the scope of the C&A process, and to not allow the scope to expand beyond a manageable effort for a system with a limited life expectancy. WinSAGA plans to be decommissioned in June 2010 and proper security controls will be implemented on the PAGE system. The PAGE system is a web-based system that will not have a distributed environment with servers across the country. Therefore, the PAGE C&A and respective System Security Plan encompasses all components of the system and accreditation boundary.
Finding #8	The draft report states that, "Even when testing was completed at Headquarters, we found that it excluded 16 percent of the security controls and control enhancements that are required by NIST for a moderate risk system."
Management's Response	Concur
Departmental Response	The WinSAGA C&A was completed in 2007, which was prior to the completion of the DOE Under Secretary of Energy Program Cyber Security Plan (PCSP) and its respective Appendix A, which documents the Office of the Under Secretary of Energy Minimum

	System Security Requirements for Unclassified Systems. Therefore, when reviewing the 2007 C&A package and respective System Security Plan (SSP), one must note that many requirements are not covered within the original package due to the fact that the DOE Under Secretary PCSP was not yet created. Additionally, a majority of the excluded security controls are identified in the System Security Plan as 'Not Applicable', and an explanation was provided for each. Most of the excluded items were related to software development or technologies that are not related to supporting WinSAGA. At the time of the C&A, there was no development work allowed for WinSAGA. For the PAGE system, the C&A package and respective SSP were created using DOE Under Secretary of Energy PCSP v 1.2, which was the most up-to-date version of the PCSP at the time of accreditation. Updates will be made to the C&A package security documentation annually and will utilize current DOE and other Federal guidance as the regulations for the review.

Communication of Security Requirements	
Finding #9	The draft report states that, "EERE Officials had not ensured that responsibility was assigned for communicating all cyber security requirements to the Information System Security Officer (ISSO) – the individual responsible for ensuring security of the information system – and system users. Specifically, the EERE Cyber Security Program Manager was the only official assigned responsibility for security over the program's systems…..Our review found that no one within EERE had been assigned the responsibility of ensuring that system specific requirements were properly communicated to the system ISSO"
Management's Response	Concur
Departmental Response	Due to a lack of resources, the EERE Cyber Security Program Manager lacks sufficient staffing to ensure separation of duties within the Cyber Security Program (CSP). While not ideal, the limited scale of the Cyber Security Program allows it to operate without the recommended segregation of duties and the principle of least privilege implemented. Additionally, although the report states that access reviews are not performed regularly and inactive accounts are not deleted, internal IV&V testing verified that all users from all user groups (HQ, PMC, and states) that have not logged in to the WinSAGA application within 183 days, will be prevented from accessing the application. For the PAGE system, EERE will look to establish greater depth of resources within the Cyber Security Program so that the EERE Cyber Security Program Manager is not the only official assigned responsibility for security over the program's systems. This will allow the CSP to meet both organizational changes and pending growth challenges improving program efficiency, overall

	communication between program stakeholders, and general collaboration.
Finding #10	The draft report states that, "We also noted that the method and approach used to validate corrective actions taken to close POA&M items was not always effective. During our review, we observed that security weaknesses existed even though the program reported them as corrected and closed."
Management's Response	Concur
Departmental Response	The report provided by the OIG contains two (2) examples of POA&M milestones that were reported as corrected and closed, while the weaknesses still existed, which were as follows: • Password configuration and complexity: Password settings were changed when the POA&M milestone was closed; however when the change was made, the WinSAGA support team erroneously assumed that the change affected all new and existing user accounts. Previously existing accounts were recently reviewed, and all PMC and State user accounts now have the same level of complexity requirements. • Appropriate storage of backups for WinSAGA: As previously noted, the POA&M issue was that the off-site storage location in Rockville was too close in proximity to the Gaithersburg office location. This was addressed by rotating off-site backups to two sites: one in Baltimore, and one in Rockville. This is a temporary solution until the EERE COOP is implemented. As a result of IG's suggestion, EERE will be designing and implementing a new POA&M Milestone/Weakness Verification process for all Headquarters systems, including WinSAGA and PAGE. EERE will have an independent verifier, review and physically verify the corrective action taken for each milestone and weakness for all Headquarter systems, prior to them being updated as "Verified" within the POA&M. This will ensure that no WinSAGA or PAGE POA&M items are closed as remediated and in place without the corrective action actually being thoroughly performed on each respective system.

IG Report No. OAS-RA-10-05

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.