DOE F 1325.8
(08-93)
United States Government

Department of Energy

Memorandum

DATE: January 28, 2008

REPLY TO ATTN OF: IG-34 (A07TG029)

Audit Report No.: OAS-L-08-04

SUBJECT: Report on "Department's Implementation of the Strategic Integrated Procurement Enterprise System – Security Planning"

TO: Chief Financial Officer, CF-1

INTRODUCTION AND OBJECTIVE

On November 28, 2007, we issued a report on *Department's Implementation of the Strategic Integrated Procurement Enterprise System – Overall Project Planning* (OAS-L-08-02). This was the second in a series of reports to address the Department of Energy's (Department) Strategic Integrated Procurement Enterprise System (STRIPES) initiative and to determine whether ongoing efforts in the areas of transition planning, interfaces, and testing; overall project planning; and security were satisfying Federal and Department system development requirements, goals, and mission needs.

In our most recent report, we observed that overall project planning for STRIPES largely satisfied Federal and Department system development requirements, goals, and mission needs. However, we noted several opportunities to improve the planning and implementation processes. To improve project management we suggested that management consolidate project documentation, approve a critical path for project execution, provide detail on duplicative systems and take action to ensure that all duplicative systems are terminated as soon as practicable. Management concurred with our suggestions and agreed to take action to resolve issues discussed in our second report. This report, the third and final in the series, focuses on whether ongoing security planning efforts are satisfying Federal and Department system development requirements, goals, and mission needs.

CONCLUSION AND OBSERVATIONS

Consistent with our last report, we noted that, for the most part, security planning for STRIPES satisfied Federal and Department system development requirements, goals and mission needs. For instance, the formal certification and accreditation process of the system had begun. Physical safeguards were also in place and if complied with, should be sufficient for controlling access to the system. Plans for continuity of operations and disaster recovery have been developed for the system. An alternate processing facility exists for recovering services and restarting operations in event of

an emergency, service disruption, or disaster. Automated controls that separate user responsibilities based on job function are in place in the system and should help ensure its integrity and that of the information that resides within. However, our review identified several opportunities to improve the security planning process.

Vulnerability Scanning

No provision exists in STRIPES planning for performing scans for vulnerabilities that are specific to the system or application on which STRIPES is based. STRIPES is hosted and managed within the Department's Application Hosting Environment (AHE), which is an enterprise hosting environment run by the Department's Office of Chief Information Officer (OCIO). The AHE manages network security and provides the necessary infrastructure to support a variety of Department business applications. According to the STRIPES security plan, scans for vulnerabilities are a common security control under the responsibility of the OCIO. An OCIO official told us that broad-based scans of the Department's network for vulnerabilities are performed monthly or when significant new vulnerabilities potentially affecting the network are identified and reported. The official also indicated that while application system specific scans could be provided if desired, they are not currently part of the service agreement for STRIPES. Such scans can be valuable for identifying application specific risk and determining the effectiveness of security controls or policy. For instance, a periodic scan could be used to assess enforcement of the 90 day password change requirement established for the system.

Encryption of Data

Officials also need to assess the risk that unencrypted transfer and storage of sensitive STRIPES data could result in compromise by unauthorized access. For risk and protection purposes, STRIPES has a moderate information sensitivity rating and will include unclassified controlled nuclear information and privacy information. According to an AHE representative supporting STRIPES, data or information is encrypted in transmission between the application server and database server. However, this data or information is not encrypted when transmitted between the database server, file storage network, and where backed up to media or tape. It is also not encrypted when residing on the database server in memory, the storage network, and backup media or tape. The data or information, therefore, could be vulnerable to unauthorized access or download from the server or storage media, or loss of backup tapes to the offsite storage location. The representative also told us that an encryption product could be installed by the OCIO that covers the database server and storage network. The AHE representative indicated that the OCIO was in the process of starting to encrypt data or information stored on tapes.

Access Controls

While a policy had been developed that largely addresses the controls necessary for managing access to the system, it needed to be updated. Specifically, we noted that the policy did not accurately reflect the method for enforcing the requirement for

changing passwords every 90 days. In addition, it did not address the timing out of sessions after a period of inactivity, additional password requirements for officials with approving authority, and the role of system owner and approvers in the semi-annual user account review process. Consistent with the objectives of the policy, a reliable and error-free methodology is essential to guarantee the integrity of information contained in STRIPES.

Contrary to Department requirements, two-factor authentication – a critical security control – had not been implemented for STRIPES accounts with privileged access. The Department's password management guidance requires implementing a mandatory two-factor authentication process for access to accounts with special privileges (e.g., system administrators). In our testing of access control configuration, we noted that the STRIPES system administrator, a privileged account holder, utilized one-factor authentication (i.e., user id and password) to access the system.

POTENTIAL IMPACTS

One of the major objectives of project officials in requesting the audit was to identify any STRIPES risks or issues that could impact the audit of financial statements. Our work up to this point to evaluate the STRIPES system development has not identified any potential issues which would impact future audits of the Department's financial statements. The issues discussed above related to security planning could, however, potentially impact the security risk to STRIPES operations and the information that will ultimately be contained within it.

SUGGESTED ACTIONS

To help ensure incorporation of sufficient protective measures, we suggest that the Chief Financial Officer direct the STRIPES project management team to:

1. Incorporate in the agreement with the OCIO provisions for performing periodic scans for vulnerabilities that are specific to the system or application on which STRIPES is based;

2. Update the STRIPES access control policy to reflect the actual controls and to clarify responsibilities for reviewing access;

3. Implement a two-factor authentication method for accessing STRIPES accounts with special privileges; and,

4. Assess the risk and recommend, if necessary, that the OCIO take actions to encrypt STRIPES data or information when transmitted, while residing in memory and when in storage onsite or at the offsite location.

MANAGEMENT REACTION

Management agreed to work with the AHE to determine if tools are available for performing scans for vulnerabilities that are specific to the system or application on which STRIPES is based. Also, they agreed to review and update the access control policy and to research the feasibility of implementing a two-factor authentication method with the STRIPES application vendor. In addition, they agreed to assess the risk and work with the OCIO to encrypt STRIPES data if determined to be required and feasible.

Since no formal recommendations are being made in this report, a formal response is not required. We appreciate the cooperation of your staff during this phase of the audit.

Rickey R. Hass
Assistant Inspector General
for Environment, Science, and Corporate Audits
Office of Inspector General

Attachment

cc: Director, Office of Management, MA-1
Chief Information Officer, IM-1
Chief of Staff
Team Leader, Audit Liaison, CF-1.2
Audit Liaison, IM-10
Audit Liaison, MA-40

Attachment

SCOPE AND METHODOLOGY

SCOPE AND METHODOLOGY

Fieldwork for Department of Energy's (Department) Implementation of the Strategic Integrated Procurement Enterprise System (STRIPES) – Security Planning was performed between July 2007 and January 2008 at Department Headquarters in Germantown, Maryland. To accomplish the audit objective, we:

- Reviewed applicable laws, regulations, and guidance pertaining to information technology; financial management systems; information and system security; and system development and implementation. We also reviewed relevant reports issued by the Office of Inspector General; Office of Cyber Security Evaluations; and the Government Accountability Office;

- Reviewed the *Government Performance and Results Act of 1993* and determined if performance measures had been established for STRIPES;

- Held discussions with Department officials and personnel and obtained and reviewed relevant documentation relating to development and implementation, particularly in the area of information and system security; and,

- Assessed the effectiveness of controls being implemented for ensuring integrity of information and safeguarding information resources from unauthorized sources.

The audit was performed in accordance with generally accepted Government auditing standards for performance audits and included tests of internal controls and compliance with laws and regulations to the extent necessary to satisfy the audit objective. Accordingly, we assessed significant internal controls and performance measures under the *Government Performance and Results Act of 1993* regarding implementation of STRIPES and found that performance measures, objectives and goals did exist relating to the STRIPES implementation effort. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our audit. We did not rely on computer-processed data to accomplish our audit objective. We discussed the contents of this report with an Office of Chief Financial Officer representative on January 14, 2008.