Summary

The Office of Inspector General (OIG) contracted with Leonard G. Birnbaum and Company, LLP (LGB), an independent certified public accounting firm, to audit the Department of State’s (Department) 2005 principal financial statements, in compliance with the Chief Financial Officers Act, as amended.1 Office of Management and Budget (OMB) Bulletin 01-02, Audit Requirements for Federal Financial Statements, requires that auditors assess the adequacy of the audited entity’s internal controls, including those on automated systems processing financial data. In addition, the auditor must determine whether an agency complies with applicable laws and regulations.2

On behalf of LGB, EWA Information and Infrastructure Technologies, Inc. (IIT), performed a vulnerability assessment of the Department’s Integrated Logistics Management System (ILMS). This work also helped LGB determine whether the Department complied with OMB Circular No. A-130,3 which requires all federal agencies to establish automated information system security programs and describes the minimum requirements for those programs.

IIT found the overall security posture of ILMS, including physical security, to be reasonable, but additional improvements are needed. The Bureau of Administration (A) had developed and documented formal operating procedures and guidelines for ILMS, including those related to access control, segregation of duties, incident response, and configuration/change management.

The general architecture for ILMS was sound, and featured protected Internet access that was monitored daily. Operating procedures and guidelines were adequate, but many remained untested. ILMS staff members understood the requirement to test all key procedures and plans, but the program had not yet progressed to the point where a specific schedule or methodology for accomplishing testing was developed.

IIT identified weaknesses related to unnecessary active services, IIT also found that A had not fully implemented the Windows Active Directory. IIT is making recommendations to address these issues. In addition, it would be beneficial for A to regularly perform unrestricted automated vulnerability scans.

Background

ILMS is the backbone of the Department’s supply-chain management process. It was implemented as a unified, web-based information system designed to upgrade the Department’s

---

1 P.L. No. 101-576.
2 In addition to the financial statement audits, OIG performs separate work to determine whether the Department complies with the Federal Information Security Management Act (P.L. No. 107-347), which requires agencies to develop agencywide security plans.
supply chain by allowing one-time data entry and shared information. ILMS was implemented in order to improve purchasing, procurement, warehousing, transportation, property management, personal effects, and diplomatic pouch and mail operations by significantly reducing the Department’s administrative burden while providing more accurate and complete financial reporting.

ILMS consists of the following commercial off-the-shelf software.

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Packaged Software Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acquisitions Management</td>
<td>Ariba Buyer and AMS Procurement Desktop Citrix Metaframe and ICA client</td>
</tr>
<tr>
<td>Materials Management</td>
<td>PeopleSoft Inventory</td>
</tr>
<tr>
<td>Transportation Management</td>
<td>PeopleSoft SCM/Inventory</td>
</tr>
<tr>
<td>Diplomatic Pouch and Mail</td>
<td>PeopleSoft SCM/Inventory</td>
</tr>
<tr>
<td>Property Management</td>
<td>PeopleSoft Asset Management</td>
</tr>
<tr>
<td>Customer Support</td>
<td>PeopleSoft Customer Relationship Management</td>
</tr>
<tr>
<td>Performance Management</td>
<td>PeopleSoft Enterprise Performance Management</td>
</tr>
<tr>
<td>Application Integration</td>
<td>SeeBeyond e*Gate</td>
</tr>
<tr>
<td>Status Tracking</td>
<td>PeopleSoft SCM</td>
</tr>
<tr>
<td>Portal</td>
<td>PeopleSoft Portal</td>
</tr>
<tr>
<td>Bar-coding</td>
<td>Symbol technologies and iLevy Data Collection Software for PeopleSoft</td>
</tr>
<tr>
<td></td>
<td>HighJump Software Asset and Data Advantage for PeopleSoft</td>
</tr>
<tr>
<td></td>
<td>Software Bar-Code Print Software</td>
</tr>
<tr>
<td>Security Tools</td>
<td>Real Secure for intrusion detection</td>
</tr>
<tr>
<td></td>
<td>Net IQ for active monitoring</td>
</tr>
<tr>
<td></td>
<td>Entrust GetAccess for identification and authentication</td>
</tr>
</tbody>
</table>

Source: Bureau of Administration.

Objectives, Scope, and Methodology

The Department has numerous systems that provide financial or performance data that are used to prepare the annual financial statements. OIG and LGB identified more than 20 financial systems that are considered significant to the preparation of financial statements. LGB, in consultation with OIG, decided to perform cyclical reviews of these systems to comply with federal auditing requirements. The Government Accountability Office agreed to this approach.

LGB chose to review ILMS during the audit of the Department’s FY 2005 principal financial statements. LGB used IIT to conduct a security vulnerability assessment of ILMS in order to determine whether vulnerabilities existed that could be exploited. IIT interviewed key personnel who manage the ILMS application and assessed the physical controls maintained in certain areas. In addition, IIT reviewed the policies and procedures related to ILMS and

---

This included an assessment of measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environments.
relevant technical documentation, including the system security authorization agreement, user documentation, and software documentation.

OIG provided a copy of the draft report to the Bureau of Information Resource Management (IRM), A, and the Bureau of Resource Management (RM) on September 6, 2006. IRM and A provided comments, which are included in their entirety as Appendices A and B, respectively. RM did not provide written comments.

Results

Overall, IIT concluded that ILMS’ security posture was reasonable. However, IIT found that there was no specific schedule or methodology for testing operating procedures and guidelines. IIT also identified three easily correctible vulnerabilities related to unnecessary active services. IIT discussed these issues with the ILMS information system security officer (ISSO) and technical support personnel and provided recommendations for addressing these weaknesses. IIT also found that A had not fully implemented the Windows Active Directory, which it believes would be beneficial. In addition, IIT concluded that if the Department’s certification and accreditation process performed on ILMS had included an unrestricted automated vulnerability scan, it would have identified the vulnerabilities identified by IIT.

Overall Security Posture

IIT found ILMS’ security posture to be reasonable, although additional improvements were needed. IIT concluded that the physical security of critical components of the supporting technical infrastructure was excellent. IIT judged the technical architecture to be sound and there were no apparent departures from established network engineering best practices. ILMS also conformed to Department standards that permitted it to benefit from security infrastructure and procedures that protected the overall network.

IIT also found that ILMS logs all connection attempts, including successful authentications, failed attempts, and attempts to log on to nonexistent or misspelled user accounts. This approach meets government and Department standards and greatly simplifies identifying and tracking suspected intrusions.
Operating Procedures and Guidelines

ILMS staff developed and documented formal operating procedures and guidelines for ILMS, including those related to access control, segregation of duties, incident response and configuration/change management. The operating procedures and guidelines appeared sound, but many remained untested. Although ILMS staff members understood the requirement to fully test all key procedures and plans, there was no specific schedule or methodology for accomplishing the task. IIT believes that the failure to conduct this essential testing was due largely to the fact that the project had not progressed to the point where sufficient time was available to perform these tests.

Recommendation 1: EWA Information and Infrastructure Technologies, Inc., recommends that the Bureau of Administration develop a timeline and methodology to fully test all Integrated Logistics Management System operating procedures and guidelines.

A agreed with this recommendation and indicated that it is working to develop a timeline and methodology for thoroughly testing and validating the effectiveness of ILMS procedures and guidelines. On the basis of A’s response, this recommendation is resolved, pending completion of this effort.

Active Services

Active services are any programs that are executed inside the network. Any installed application or system could include unnecessary active services. Users are not always aware that these programs are running. Sometimes these programs act as a gateway into the computer for external devices. Systems administrators should only open needed services and ports because each active service and opened port represents a potential point of attack for penetrating an application.

IIT identified numerous instances in ILMS where system administrators were not aware of or appropriately managing active services. These services not only related to newly installed applications, but also some services related to applications that had been removed from the system. ILMS administrators should actively manage the programs on their system. If an active service is not needed, then it should be disabled.

Recommendation 2: EWA Information and Infrastructure Technologies, Inc., recommends that the Bureau of Administration develop a process to actively identify and disable unnecessary services on the Integrated Logistics Management System.

Both IRM and A indicated that efforts have been taken to limit the use of unnecessary services and requested additional information on the issues identified by IIT concerning these services. IIT provided details of all of the technical findings to the ISSOs and application managers at the time of the assessment. For instance, IIT found that Compaq Insight Manager, a very powerful service/application that is installed by default on Compaq servers, was running on one port in several hosts. Because of steps IRM and A are taking to limit the use of unnecessary
services, OIG is resolving this recommendation. OIG will close it once IRM and A provide information showing that they have addressed the additional unnecessary services identified during the assessment.

**Patch Management**

When vendors identify performance problems or security vulnerabilities, they develop new software code to correct the problems and vulnerabilities. These software corrections are referred to as patches.
Recommendation 4: Windows Active Directory

Windows Active Directory

ILMS is set up in a client-server configuration. However, the Department has not fully implemented Windows Active Directory for this application. Active Directory is a central component of the Windows platform that provides the means to manage the identities and relationships that make up network environments. By creating a link between user accounts, mailbox accounts, and applications, Active Directory simplifies the task of adding, modifying, and deleting user accounts.

A’s ability to manage and track ILMS user activity would be significantly enhanced if Windows Active Directory was fully deployed. For instance, Windows Active Directory would allow A to manage and track ILMS user activity by assigning each user specific access rights to ILMS, and logging that access. Windows Active Directory also includes useful security tools, including log tracking, intruder alert, policy enforcement, and patch update status, that can help administrators better understand the operations of the network and proactively address network problems, errors, or concerns.

Recommendation 5: Certification and Accreditation

As part of its ongoing information system security program, the Department certified and accredited ILMS on June 15, 2005. The certification and accreditation process did not include an unrestricted automated vulnerability scan of the system according to the supporting documentation IIT reviewed. By conducting this type of scan, IIT identified a number of the weaknesses discussed above. IIT believes that if A were to perform periodic scans of ILMS, it would be able to identify and address the types of vulnerabilities that IIT identified in this report.
Recommendation 6: EWA Information and Infrastructure Technologies, Inc., recommends that the Bureau of Administration periodically conduct unrestricted vulnerability scans of the Integrated Logistics Management System in coordination with the appropriate Department entities.

Both IRM and A agreed with the recommendation. IRM indicated that it currently employs vulnerability scanning tools not previously on hand when ILMS was certified and accredited. In addition, the Department is working to fully implement an enterprise tool that will scan continuously. A indicated that it would investigate the possibility of coordinating regular vulnerability scans with IRM. On the basis of A’s and IRM’s response, this recommendation is resolved, pending completion of this effort.
UNCLASSIFIED

MEMORANDUM

TO: OIG – Mr. Howard J. Krongard

FROM: IRM – Charles D. Wisecarver, Acting


Thank you for the opportunity for us to address comments to the subject report. Our responses are attached.
Recommendation 1: EWA Information and Infrastructure Technologies, Inc., recommends that the Bureau of Administration develop a timeline and methodology to fully test all Integrated Logistic Management System operating procedures and guidelines.

IRM Response: IRM has no comments.

Recommendation 2: EWA Information and Infrastructure Technologies, Inc., recommends that the Bureau of Administration develop a process to actively identify and disable unnecessary services on the Integrated Logistics Management System.

IRM Response: Department of State Security Configuration Standards include provisions intended to limit the use of unnecessary services. Without a list of those services identified by IIT as unnecessary, we cannot comment on this recommendation.

Recommendation 3: EWA Information and Infrastructure Technologies, Inc., recommends that the Bureau of Administration in conjunction with the Chief Information Officer, fully implement Active Directory in the Integrated Logistics Management System to manage and track activity throughout the network.

IRM Response: Several applications have been linked with Active Directory as outlined in Recommendation 5. This linkage has proven successful and beneficial, providing the advantages outlined in the recommendation as well as single sign-on, and the number of applications taking this approach continues to grow. The approach is implemented when the application owners generate the linkage within their application (through program calls) and Windows Active Directory. While IRM stands ready to assist with technical advice, testing, etc.,
this would require A Bureau taking the lead in making the required changes to ILMS.

**Recommendation 6:** EWA Information and Infrastructure Technologies, Inc., recommends that the Bureau of Administration periodically conduct unrestricted vulnerability scans of the Integrated Logistics Management System in coordination with the appropriate Department entities.

**IRM Response:** The Department of State’s information security evaluation entities currently employ vulnerability scanning tools not previously on hand when ILMS was certified and accredited. In addition to the use of these tools during C&A, the Department is working to fully implement an enterprise tool that will scan continuously. We believe this resolves this recommendation.
MEMORANDUM

TO: OIG – Howard J. Krongard
FROM: A/LM/PMP – Cecilia Coates
SUBJECT: Response to Draft Information Technology Vulnerability Assessment of the Integrated Logistics Management System (AUD/FM-06-XX)

A/LM has reviewed the draft Information Technology Vulnerability Assessment of the Integrated Logistics Management System. Since the audit the Office of Logistics Management (A/LM) has made many improvements to the overall Integrated Logistics Management System (ILMS) posture. Many of the concerns identified by IIT have been addressed and plans are being developed to mitigate the issues. The Bureau of Administration Office of Logistics Management (A/LM) agrees with IIT’s findings and recommendations except recommendation three (3). Comments are provided below.

**Recommendation 1:** EWA Information and Infrastructure Technologies, Inc., recommends that the Bureau of Administration develop a timeline and methodology to fully test all Integrated Logistics Management System operating procedures and guidelines.

A/LM is working to develop a timeline and methodology for thoroughly testing and validating the effectiveness of ILMS procedures and guidelines.

**Recommendation 2:** EWA Information and Infrastructure Technologies, Inc., recommends that the Bureau of Administration develop a process to actively identify and disable unnecessary services on the Integrated Logistics Management System.
A/LM made every effort to configure the ILMS environment in accordance with DoS Security Configuration Standards. The ILMS accreditation boundary was subjected to the most comprehensive security evaluation methods applied within the Department of State’s Systems Authorization Process. The DoS Security Configuration Guides are intended to limit the use of unnecessary services. A/LM has made significant efforts to limit the presence of unnecessary services running within ILMS. A/LM requests a more specific description of the instances identified by IIT concerning these services to facilitate the review and remediation of the issues.

**Recommendation 3:**

Recommendation 4:

Recommendation 5: EWA Information and Infrastructure Technologies, Inc., recommends that the Bureau of Administration, in conjunction with the Chief Information Officer, fully implement Active Directory in the Integrated Logistics Management System to manage and track activity throughout the network.
The Bureau of Information Resources Management (IRM), and the Office of the Chief Information Officer, is fully engaged with the deployment of Active Directory to all entities within the Department of State. A/LM anxiously awaits the full implementation of Active Directory services and will integrate them with A systems once available. Furthermore, IRM and A are in the process of consolidating IT services. A/LM anticipates that this consolidation initiative will substantially improve all facets of systems maintenance to include the deployment of those security tools and capabilities native to Active Directory services. As of June 2006 A/LM migrated all but one ILMS server to Active Directory.

**Recommendation 6:** EWA Information and Infrastructure Technologies, Inc., recommends that the Bureau of Administration periodically conduct unrestricted vulnerability scans of the Integrated Logistics Management System in coordination with the appropriate Department entities.

A/LM is aware of the need for vulnerability scanning and shares IIT’s concern. It is our understanding that IRM/IA and DS are addressing this issue and close to finalizing the implementation of such tools. Tenable has been identified as one of the tools to be used and is currently awaiting ITCCB approval. A/LM together with A Bureau will investigate the possibility of coordinating regular vulnerability scans with IRM/IA and DS.