

UNCLASSIFIED

Information Technology Vulnerability Assessment of the Integrated Logistics Management System

AUD/FM-07-06, November 2006

Important Notice

~~This report is intended solely for the official use of the Department of State or any agency receiving the report directly from the Office of Inspector General. No secondary distribution may be made outside the Department of State or by other agencies or organizations in whole or in part, without prior authorization by the Inspector General. Public availability of the document will be determined by the Inspector General under the U.S. Code 5 U.S.C. 552. Improper disclosure of this report may result in criminal, civil, or administrative penalties.~~

UNCLASSIFIED

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, (b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) 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.

³ *Management of Federal Information Resources*, Appendix III, Security of Federal Automated Resources.

UNCLASSIFIED

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 1: ILMS’ Commercial Off-the-Shelf Software

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

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.⁴ In addition, IIT reviewed the policies and procedures related to ILMS and

⁴ This included an assessment of measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environments.

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.

(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)

Recommendation 3: (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)

(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)

Recommendation 4: (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)

(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

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

A and IRM both agreed with this recommendation. A indicated that it is in the process of implementing Active Directory on all of its servers. On the basis of A’s and IRM’s response, this recommendation is resolved, pending completion of this effort.

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

Appendix A



United States Department of State


Washington, D.C. 20520

OCT - 6 2006

UNCLASSIFIED

MEMORANDUM

TO: OIG – Mr. Howard J. Krongard

FROM: IRM – Charles D. Wisecarver, Acting 

SUBJECT: IRM Comments on the *Information Technology Vulnerability Assessment of the Integrated Logistics Management System* (AUD/FM-06-XX)

Thank you for the opportunity for us to address comments to the subject report. Our responses are attached.

RECEIVED
OIG/ISP
2006 OCT 26 P 12: 22

UNCLASSIFIED

UNCLASSIFIED

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.



United States Department of State

Washington, D.C. 20520

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: (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

Recommendation 4: (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

Recommendation 5: EWA Information and Infrastructure Technologies, Inc., recommends that the Bureau of Administration, in junction 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.