

**Information Technology Assessment
of the Consolidated American Payroll Processing System**

AUD/FM-07-35

April 2007

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.~~

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) 2006 principal financial statements, in compliance with the Chief Financial Officers Act, as amended.¹ Office of Management and Budget (OMB) Bulletin 06-03, *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 an assessment of the Consolidated American Payroll Processing System (CAPPS). 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.

The majority of CAPPS processing is performed at the Global Financial Services (GFS) Center in Charleston, South Carolina. CAPPS and the Regional Financial Management System (RFMS) share a user environment at the GFS Center. This user environment was evaluated during IIT's vulnerability assessment of RFMS.⁴ Outside of the GFS Center in Charleston, there is one small CAPPS user enclave in the Washington, D.C. area.

Because of the recent RFMS technical vulnerability assessment at the GFS Center in Charleston and the small number of additional users in the Washington, D.C. area, IIT did not conduct a formal technical vulnerability assessment. The findings included in the RFMS report are also applicable to CAPPS. IIT did note that the Washington-area CAPPS users benefited from a full Microsoft Active Directory implementation, which was not the case at the GFS Center in Charleston. During its limited assessment of CAPPS and its components, IIT did not identify any additional significant weaknesses that had not already been included in the RFMS report.

Background

CAPPS generates payments to all U.S. citizen employees of the Department and certain other agencies who use the Department to provide payroll services. The system is used to make payments to Foreign Service and Civil Service employees, and personal services contractors

¹ Pub.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 (Pub.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.

⁴ *Information Technology Vulnerability Assessment of the Regional Financial Management System* (AUD/FM-07-13, Feb. 2007.)

(PSC), all of whom are subject to U.S. legislation and federal pay plans. It excludes foreign nationals, who are paid by decentralized systems.

CAPPS is a legacy mainframe application that is considered a mission-critical system. The system is housed in the Main State Data Center. Disaster recovery capabilities are supported at the Beltsville Information Management Center. CAPPS benefits from security processes and tools that protect the mainframe infrastructure. CAPPS users are concentrated primarily at the GFS Center in Charleston, but a small number of additional users is located in the Washington, D.C., area.

CAPPS is a business application that operates on a mainframe-based, centralized, client server processing model. This model is designed to support remote access rather than distributed processing. The CAPPS current and historical master files constitute the central repository of American personnel and payroll information. The centralized payroll staff makes payroll changes and time and attendance (T&A) adjustments via CAPPS.

CAPPS underwent a certification and accreditation (C&A) assessment in July 2004. After completion of the C&A, CAPPS was granted an initial 18-month authority to operate on July 13, 2004, and was granted an 18-month extension. The Department is preparing to update the C&A in July 2007.

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 CAPPS during the audit of the Department's FY 2006 financial statements. LGB used IIT to assess technical information technology controls related to CAPPS. CAPPS and RFMS share a user environment at the GFS Center. This user environment was evaluated during IIT's vulnerability assessment of RFMS, which was done as part of the audit of the FY 2005 financial statements. Therefore, IIT did not perform a technical vulnerability assessment of key systems related to the CAPPS application during this work. IIT limited its work to interviewing key personnel who manage the CAPPS application and assessing the physical controls maintained in certain areas.⁵ In addition, IIT reviewed the policies and procedures related to RFMS and 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 Resource Management (RM) and the Bureau of Information Resource Management (IRM) on February 27, 2007. RM and IRM did not provide comments on this report.

⁵ This included an assessment of measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environments.

Results

During the audit of the Department's FY 2005 financial statements, IIT conducted a technical assessment of the information technology infrastructure for RFMS and found that the overall security posture of RFMS needed improvement. IIT found that RM had disabled important logging functions, had not fully implemented the Windows Active Directory, had allowed unnecessary active services on the application, did not implement patches in a timely manner, and was not appropriately managing default configurations. As noted, CAPPS and RFMS share a user environment at the GFS Center. The findings included in IIT's report on the information technology vulnerability assessment of RFMS are also applicable to CAPPS.

During its limited assessment of CAPPS and its components, IIT did not identify any additional significant weaknesses that had not already been reported as part of the assessment of RFMS. IIT concluded that the overall security posture of the CAPPS application was adequate. IIT found that the CAPPS operating procedures were reasonable, the information systems security officer (ISSO) was effectively monitoring CAPPS, and RM was appropriately preparing for the upcoming C&A of the CAPPS application.

Operating Procedures and Guidelines

Policies and procedures are an integral part of an internal control environment. RM has reasonable, written operating procedures and guidelines for CAPPS access controls, segregation of duties, incident response, and configuration and change management. Many of the key operating procedures and guidelines that are relevant to CAPPS are specifically associated with the Department's mainframe operating environment and infrastructure.

Access Controls

The CAPPS ISSO manages access controls. The ISSO authorizes user access to CAPPS, including privilege level, through a manual paper process. The ISSO sends the written approvals for access to the mainframe security team, which is the only entity authorized to create user accounts. The ISSO periodically reviews active accounts to ensure their continued validity. The ISSO also periodically reviews the CAPPS activity logs to determine the existence of unusual use patterns or other potential security events. The ISSO has been granted remote access to the mainframe environment, and is therefore capable of responding rapidly to security issues or other problems that occur during nonduty hours. IIT found that this process was working effectively. Allowing the ISSO to have constant availability to the system in case of an emergency or security incident is a strong control.

Certification and Accreditation

As part of its ongoing information system security program, after completion of a C&A effort, the Department issued an authority to operate for CAPPS on July 13, 2004. The initial authorization was for 18 months. Owing to changes in the Department's C&A requirements, an

18-month extension of the authority to operate was granted on January 5, 2005. This authority expires on July 31, 2007.

IIT noted that RM has improved its oversight process by assigning RM staff with specific responsibilities related to the C&A process. The individuals assigned these responsibilities directly manage overall C&A planning and execution and have already begun preparing for the next CAPPS C&A, which is scheduled for July 2007. These individuals are also responsible for conducting formal, annual self-assessments of all RM managed systems. IIT reviewed some of the self-assessments performed on CAPPS and found them to be thorough. These self-assessments were conducted under the procedures defined in the National Institute of Standards and Technology's Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*.