

UNCLASSIFIED

**Information Technology Vulnerability Assessment
of the Regional Financial Management System**

AUD/FM-07-13

February 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.~~

UNCLASSIFIED

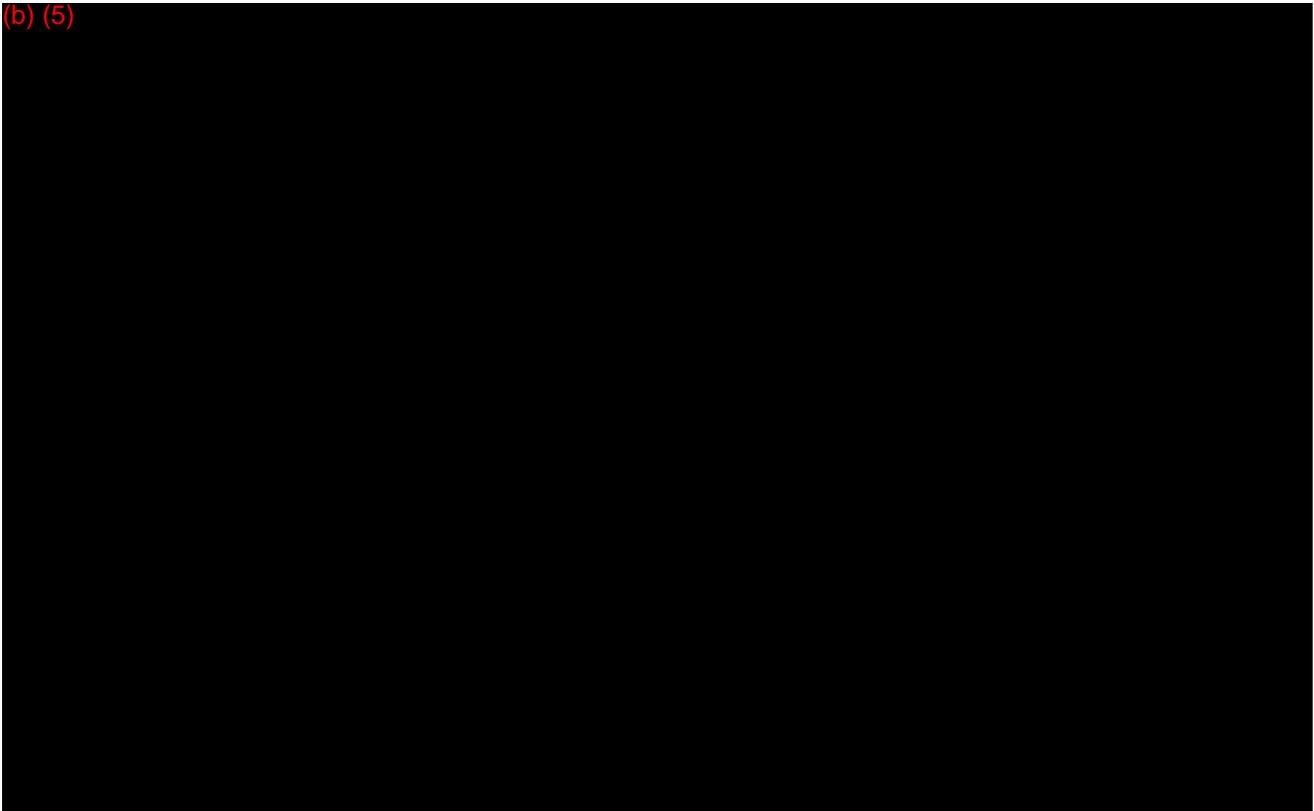
UNCLASSIFIED

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 Regional Financial Management System (RFMS). This work also helped LGB determine whether the Department had 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.

(b) (5)



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

Background

RFMS is the financial management and disbursing system used at the Global Financial Services (GFS) Centers. RFMS consists of four discrete components:

- RFMS/M, which is the Momentum application, a commercial off-the-shelf accounting system that is certified by the Joint Financial Management Improvement Program.
- RFMS/D, which is the disbursing component of RFMS hosted at both GFS Charleston and GFS Bangkok. This component was developed by the Department to meet the requirements of disbursing in multiple foreign currencies.
- RFMS/R, which contains a RFMS accounting database optimized for reporting, queries, and data extraction.
- RFMS/R Viewer, which allows local viewing of relevant data.

The Department conducted a full certification and accreditation test of RFMS, including a Security Test and Evaluation, and gave it an 18-month authority to operate on July 6, 2005. A 36-month authority was not granted because the Department had not conducted penetration testing as part of the process.

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 RFMS during the audit of the Department's FY 2005 principal financial statements. LGB used IIT to conduct a security vulnerability assessment of RFMS in order to determine whether vulnerabilities existed that could be exploited. IIT interviewed key personnel who manage the RFMS application and assessed the physical controls maintained in certain areas.⁴ 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.

IIT also performed a technical vulnerability assessment of key systems on the RFMS subnet using an automated vulnerability-scanning tool. The test included a series of custom applications designed to determine whether an attacker could exploit the identified vulnerabilities. IIT installed the automated tools on a laptop computer connected to the GFS

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

UNCLASSIFIED

Charleston network that supports RFMS to gather relevant configuration and other data from hosts throughout the network. IIT then compared the collected data against a continuously updated database that determines whether there are vulnerabilities against specific known threats.

OIG provided a copy of the draft report to RM and the Bureau of Information Resource Management (IRM) on October 10, 2006. RM and IRM provided comments, which are included in their entirety as Appendices A and B, respectively.

Results

(b) (5)



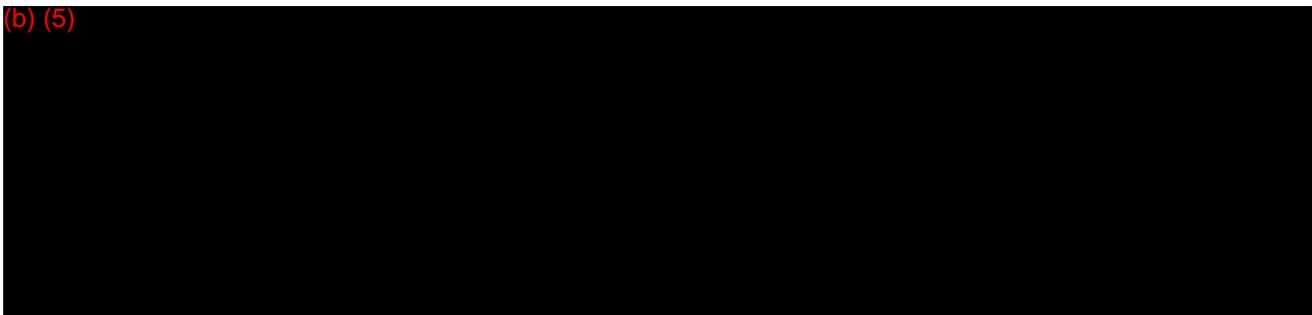
Operating Procedures and Guidelines

RM had not completed developing formal operating procedures and guidelines for RFMS access controls, segregation of duties, incident response, and configuration/change management. Policies and procedures are an integral part of an entity's internal control environment.

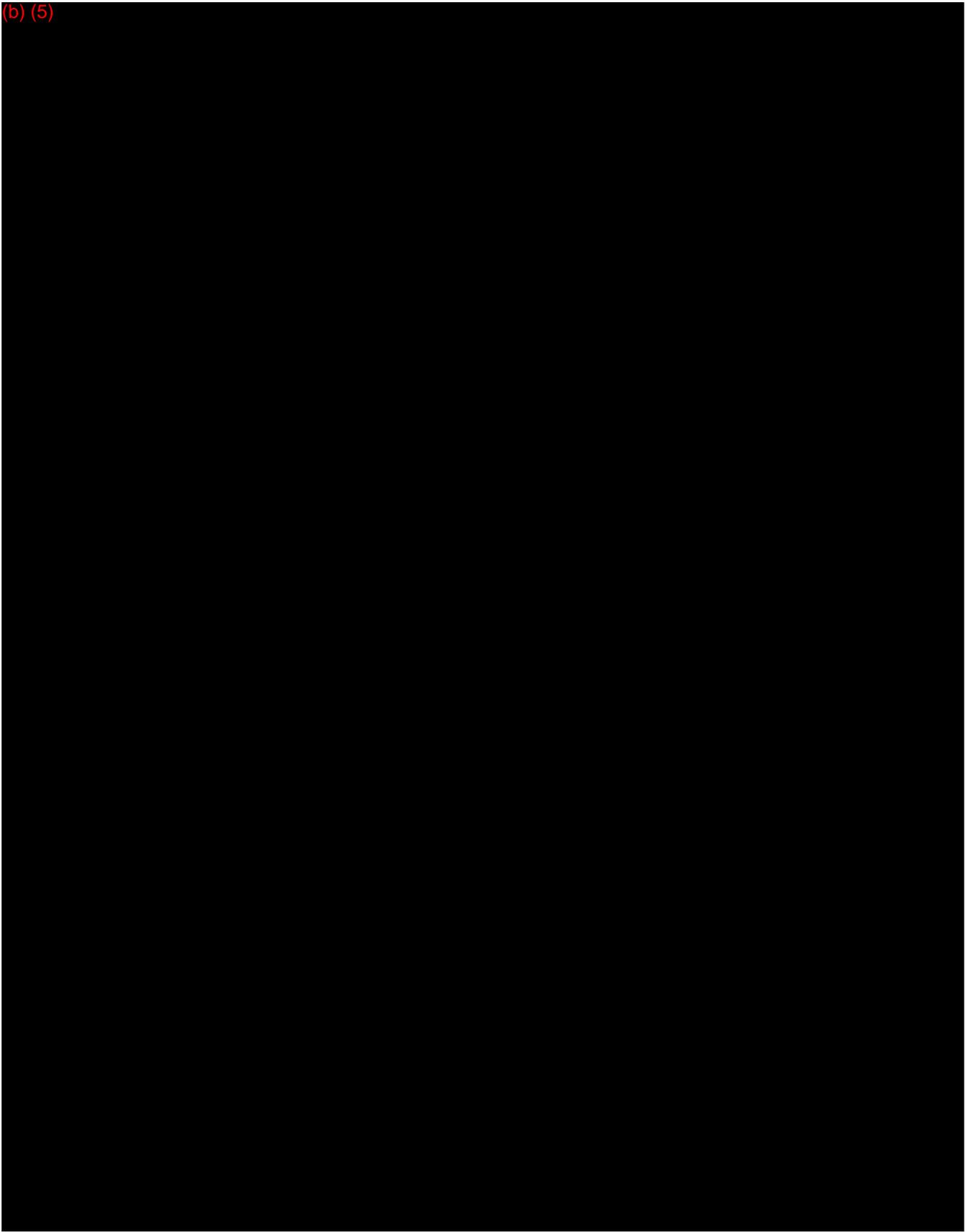
Recommendation 1: EWA Information and Infrastructure Technologies, Inc., recommends that the Bureau of Resource Management develop useful and complete operating procedures and guidelines for the Regional Financial Management System.

RM indicated that it has developed detailed processes, process descriptions, and quality work instructions/guidelines for RFMS. On the basis of RM's response, this recommendation is resolved. This recommendation can be closed once RM provides copies of formal operating procedures related to access controls, segregation of duties, incident response, and configuration/change management.

(b) (5)

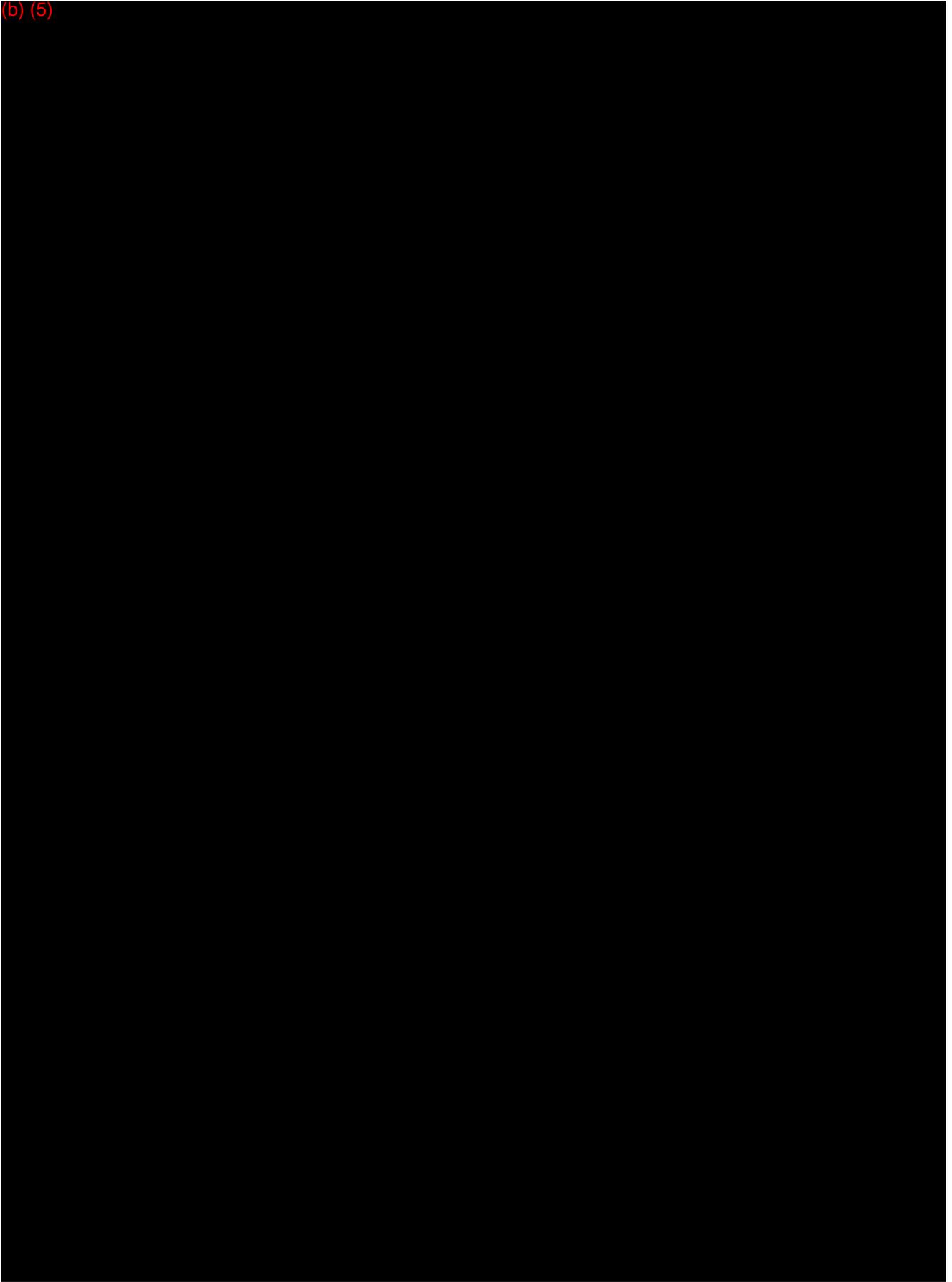


(b) (5)



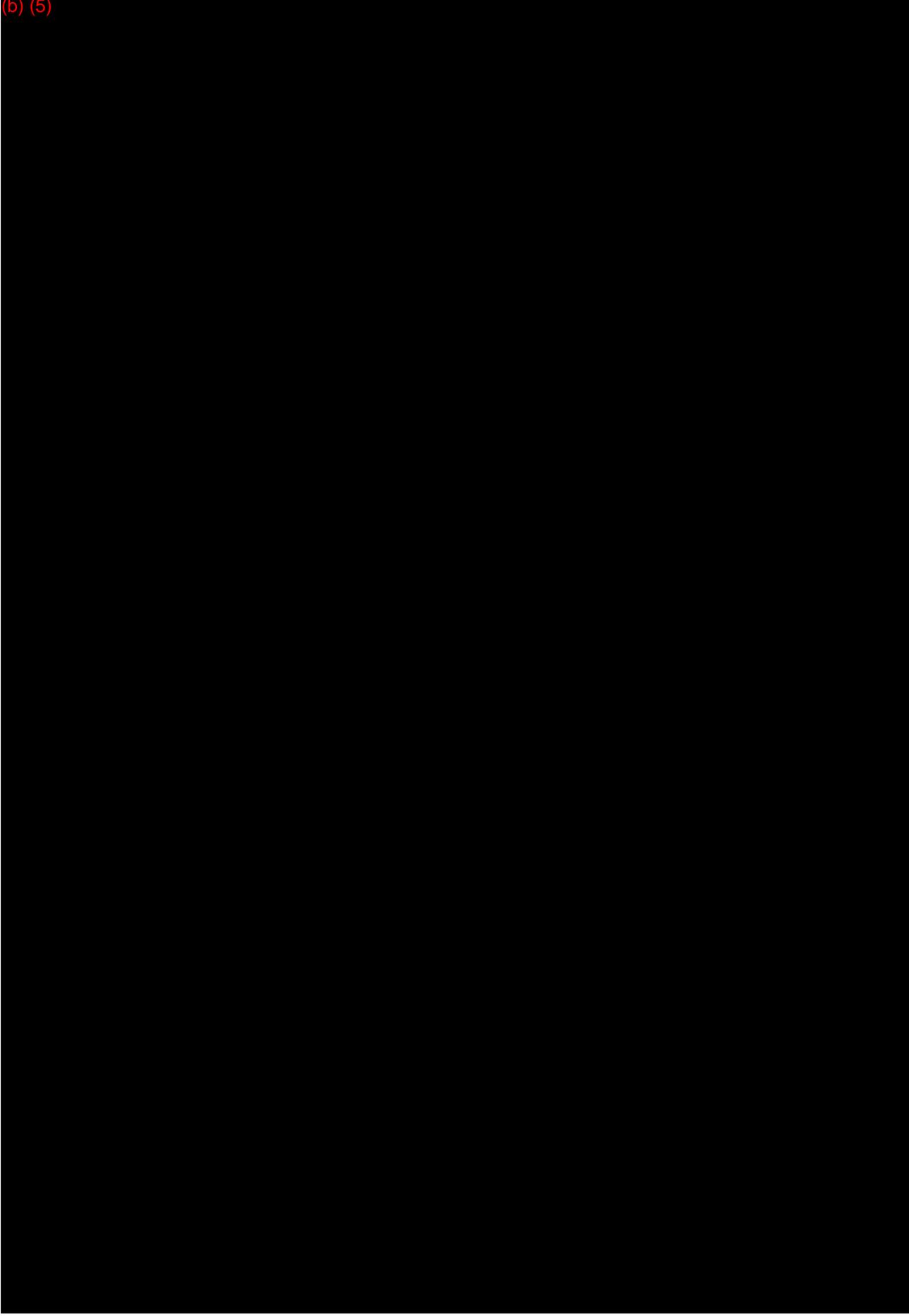
UNCLASSIFIED

(b) (5)

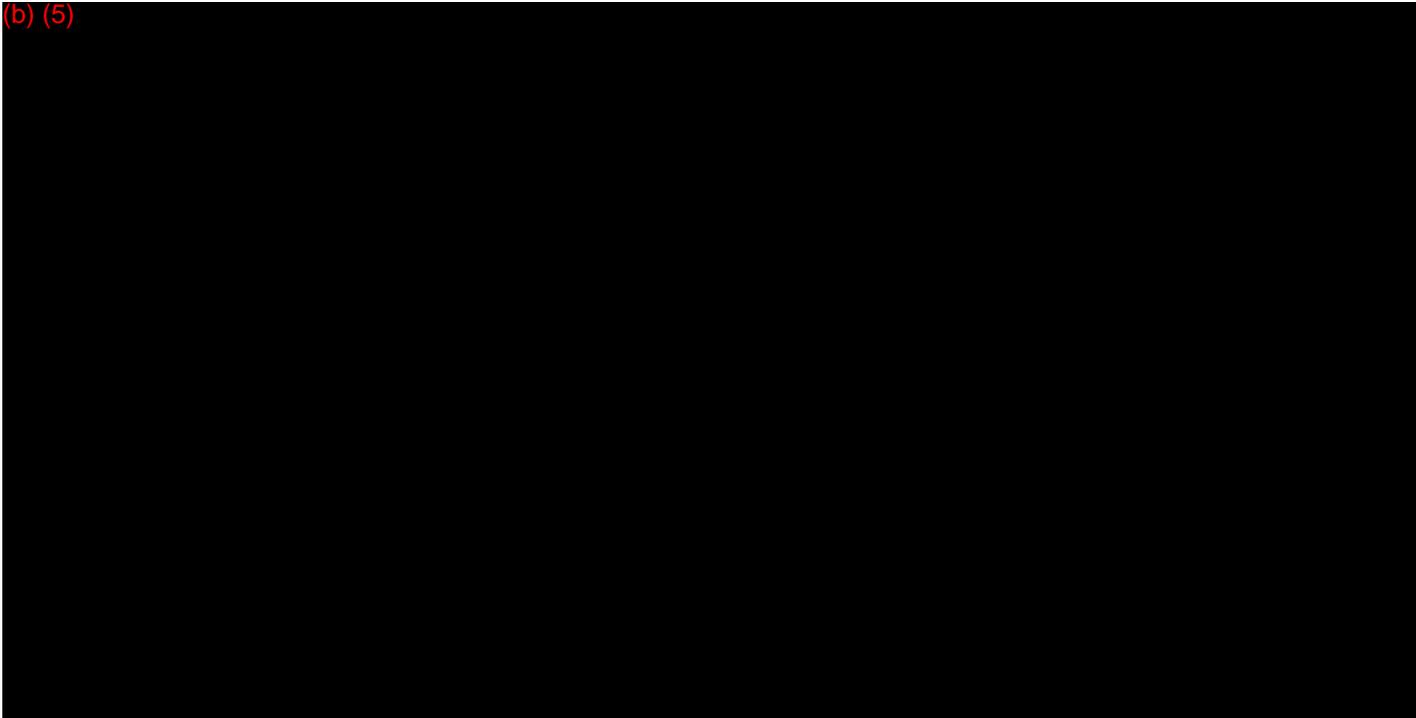


UNCLASSIFIED

(b) (5)



(b) (5)





United States Department of State
*Assistant Secretary for Resource Management
and Chief Financial Officer*
Washington, D.C. 20520

JAN 4 2007

UNCLASSIFIED

MEMORANDUM

TO: OIG Howard J. Krongard

FROM: RM – Bradford R. Higgins *BRH*

SUBJECT: Information Technology Vulnerability Assessment of the Regional
Financial Management System (OIG Report Number AUD/FM-07-
XX)

I endorse and am forwarding the comments contained in the attached response to
the subject OIG correspondence.

Attachment:

Memorandum dated December 18, 2006 Information Technology Vulnerability
Assessment of the Regional Financial Management System (OIG Report Number
AUD/FM-07-XX).

Cleared:

Philip Schlatter, RM/EX

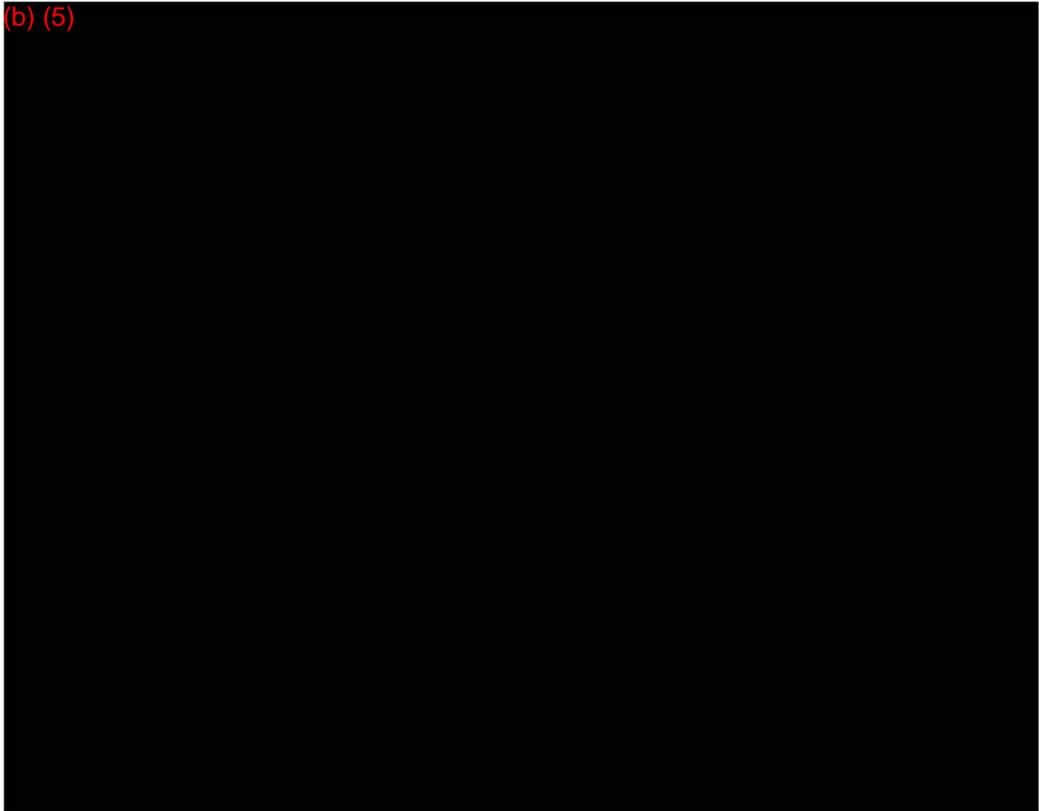
Christopher Flaggs, RM/DCFO

Draft Report on the Information Technology Vulnerability Assessment
of the Regional Financial Management System
(AUD/FM-07-XX)

Recommendation 1: EWA Information and Infrastructure Technologies, Inc., recommends that the Bureau of Resource Management develop useful and complete operating procedures and guidelines for the Regional Financial Management System.

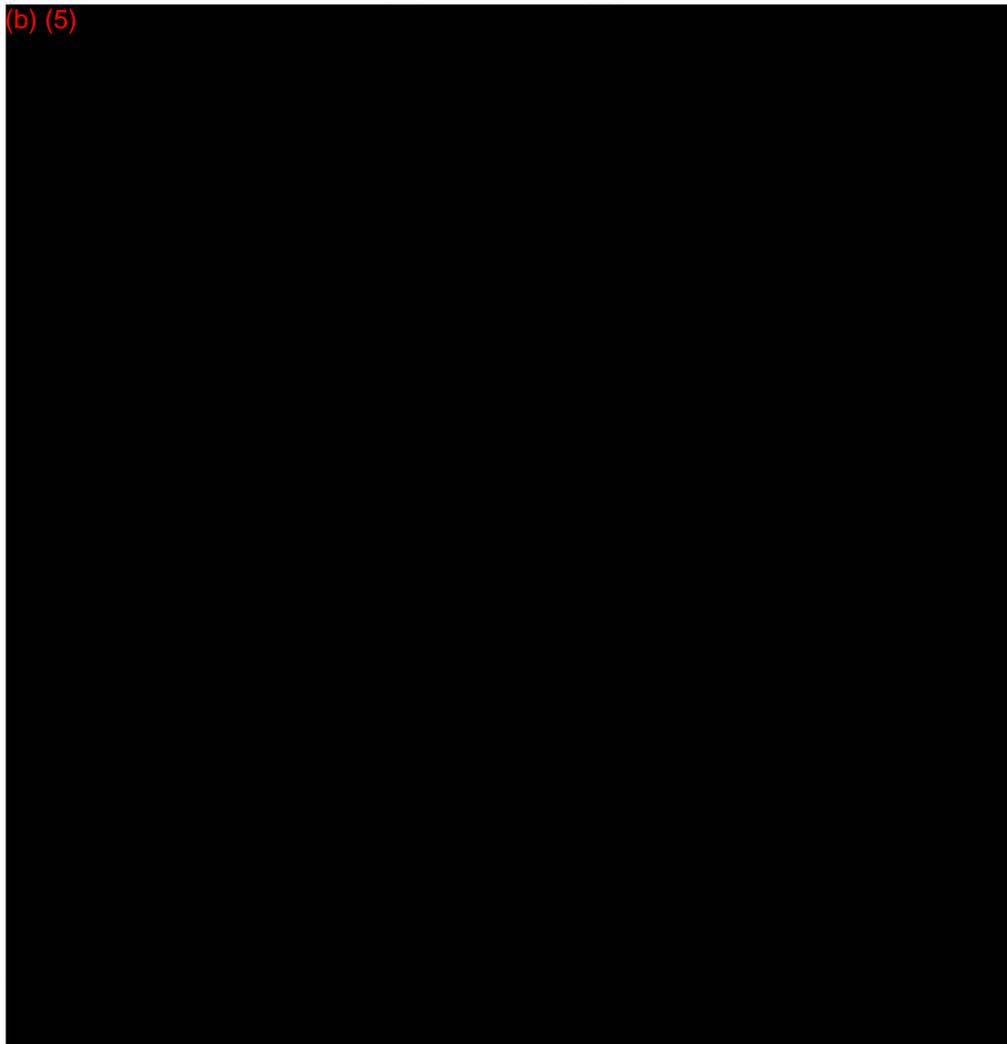
RM Response: GFSC has developed detailed processes, process descriptions, and quality work instructions/guidelines for RFMS.

(b) (5)



Draft Report on the Information Technology Vulnerability Assessment of the
Regional Financial Management System
(AUD/FM-07-XX)

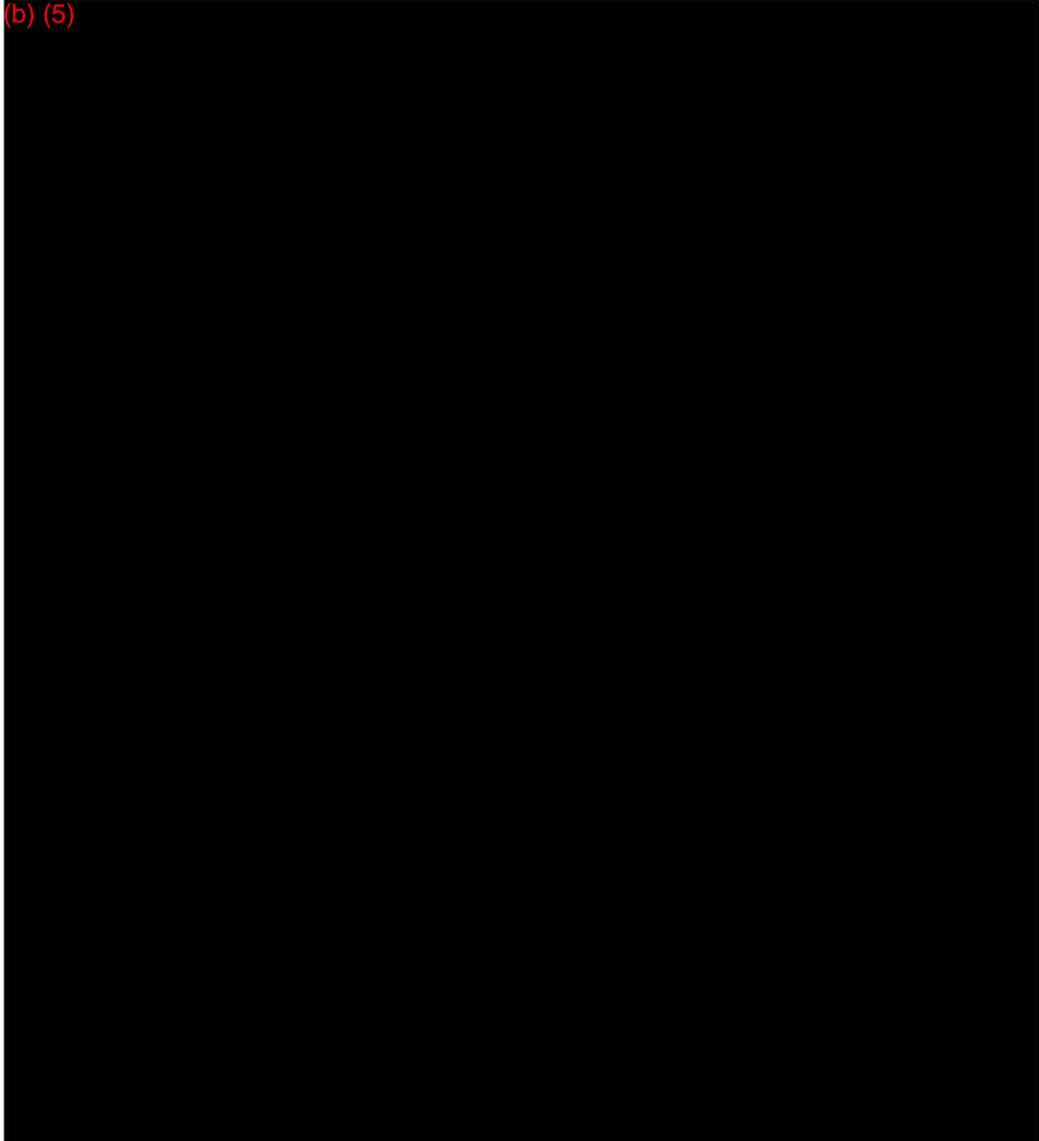
(b) (5)



-3-

Draft Report on the Information Technology Vulnerability Assessment of the
Regional Financial Management System
(AUD/FM-07-XX)

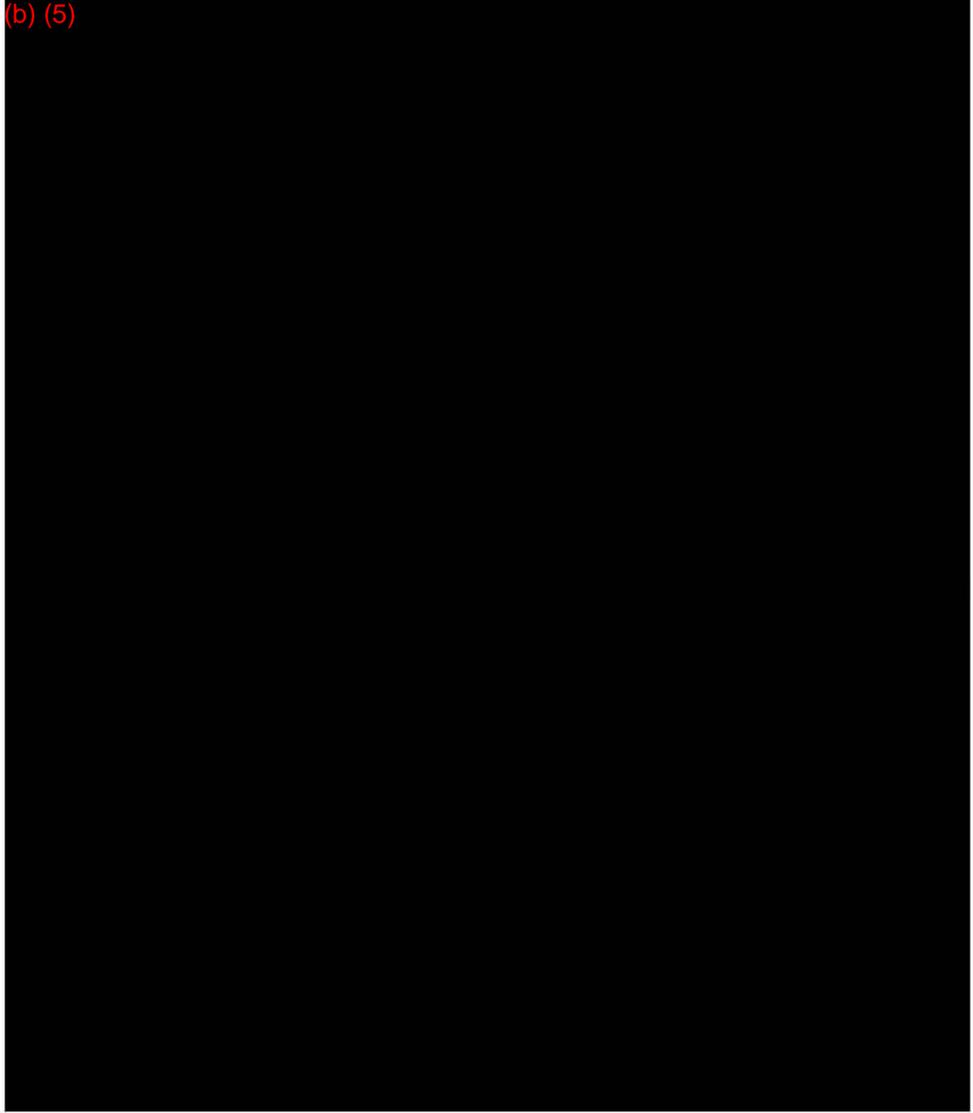
(b) (5)



-4-

Draft Report on the Information Technology Vulnerability Assessment of the
Regional Financial Management System
(AUD/FM-07-XX)

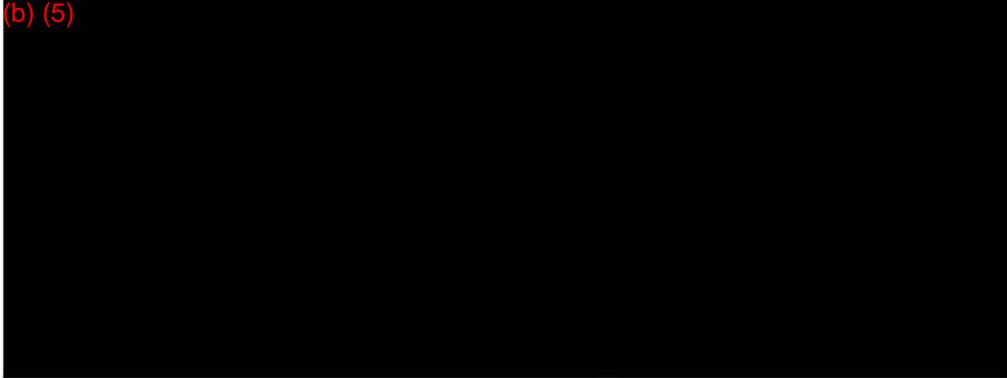
(b) (5)



-5-

Draft Report on the Information Technology Vulnerability Assessment of the
Regional Financial Management System
(AUD/FM-07-XX)

(b) (5)





U.S. DEPARTMENT OF STATE

WASHINGTON, D.C. 20520

October 25, 2006

MEMORANDUM

TO: OIG – Mr. Howard J. Krongard

FROM: IRM/BPC/EAP/PAS – Daniel Sheerin *DS*

SUBJECT: IRM Comments on the *Information Technology Vulnerability Assessment of the Regional Financial Management System* (AUD/FM-07-XX)

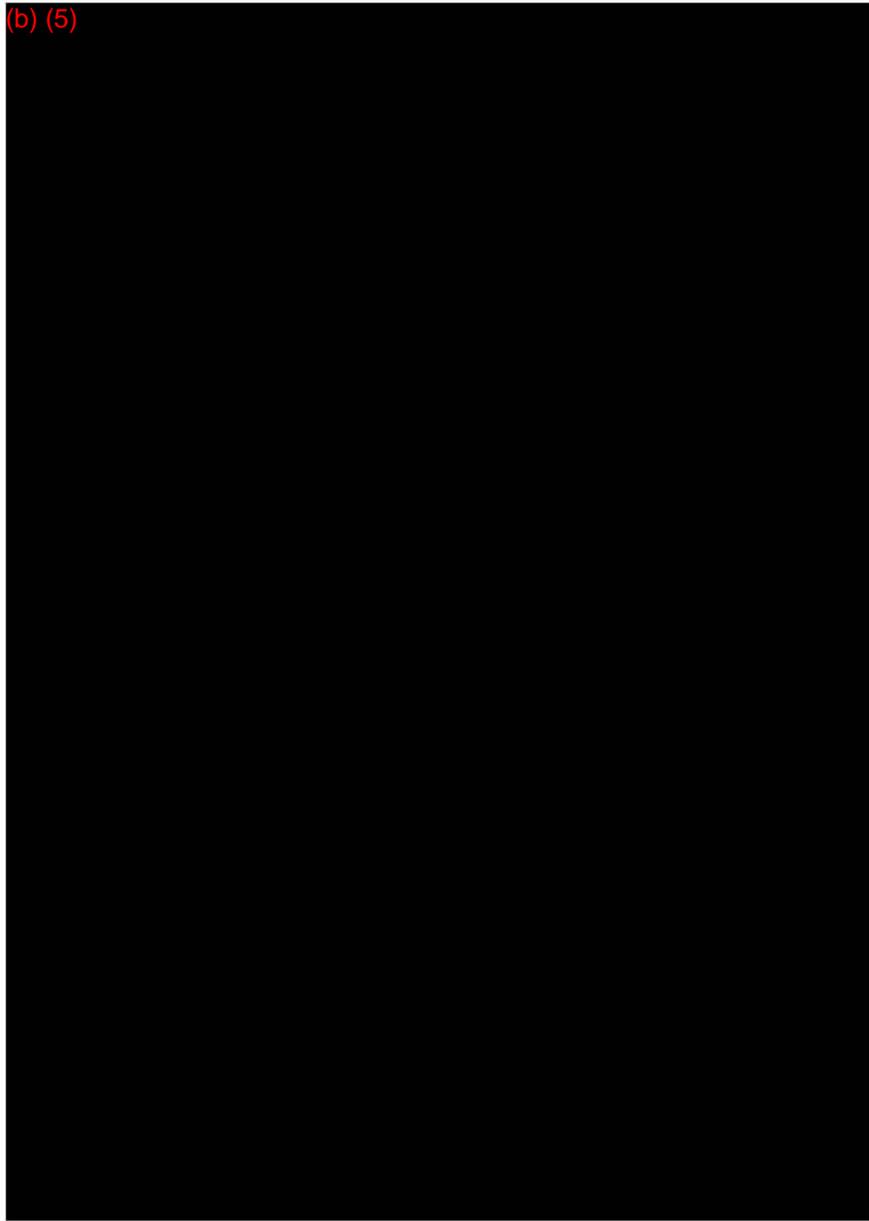
REF: Your Memo dated October 10, 2006, same subject

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 Resource Management develop useful and complete operating procedures and guidelines for the Regional Financial Management System.

IRM Response: No comment.

(b) (5)



(b) (5)



FRAUD, WASTE, ABUSE, OR MISMANAGEMENT
of Federal programs
and resources hurts everyone.

Call the Office of Inspector General
HOTLINE
202-647-3320
or 1-800-409-9926
or e-mail oighotline@state.gov
to report illegal or wasteful activities.

You may also write to
Office of Inspector General
U.S. Department of State
Post Office Box 9778
Arlington, VA 22219
Please visit our Web site at:
<http://oig.state.gov>

Cables to the Inspector General
should be slugged "OIG Channel"
to ensure confidentiality.