audit
report

Issue Date:
February 14, 2006

Audit Report Number:
2006-DP-0004

TO: Lisa Schlosser, Chief Information Officer, A

FROM: Hanh Do

Hanh Do, Director, Information System Audit Division, GAA

SUBJECT: Review of HUD's Information Security Program

HIGHLIGHTS

What We Audited and Why

We audited the U.S. Department of Housing and Urban Development's (HUD) information security program compliance with federal requirements. We evaluated (1) the adequacy of the categorization of HUD major systems, (2) whether HUD's Office of the Chief Information Officer has developed security policies and implemented and monitored enterprisewide controls, and (3) whether HUD program officials and system owners have properly implemented information security responsibilities assigned to them. We performed this audit as a component of our fiscal year 2005 consolidated financial statements audit and our annual evaluation of HUD's information system security program in the context of the Federal Information Security Management Act.

What We Found

HUD has made considerable progress in implementing a comprehensive, entitywide information system security program. However, our review noted several matters that require management attention: (1) HUD's program offices and system owners have not properly categorized HUD's application systems and utilities, which could result in unnecessary expenditure of funds; (2) HUD's Office of the Chief Information Officer has not fully implemented an effective entitywide information security program; and (3) HUD's program offices and system owners have not complied with security responsibilities in accordance with the Federal Information Security Management Act and HUD information security program requirements.

What We Recommend

1. We recommend that the Office of the Chief Information Officer
   - Establish a HUD-wide process to review and categorize information and information systems in accordance with the Federal Information Processing Standards and the National Institute of Standards and Technology Special Publication 800-60.
   - Complete the design and implementation of a compliant information security program to include policies and procedures for an inventory of information systems, a role-based security information security training program, and systems interconnectivity.
   - Develop and test contingency plans in accordance with federal requirements and HUD information technology policies.

2. We recommend that the Office of the Chief Information Officer request that the Deputy Secretary direct program officials to
   - Categorize their information systems in accordance with Federal Information Processing Standards and National Institute of Standards and Technology Special Publication 800-60.
   - Ensure that information system owners participate in a role-based training program that provides the information security training needed to ensure information system compliance with federal and HUD requirements.
   - Comply with federal and HUD requirements by participating in the development and implementation of security documents and projects; implementing protections for system security vulnerabilities identified; establishing system interconnection; and including federal information security requirements in its contracts and management processes.

Auditee’s Response

The Office of the Chief Information Officer concurs with the contents and recommendations detailed in the report. The complete text of the auditee’s response can be found in appendix B.

TABLE OF CONTENTS

BACKGROUND AND OBJECTIVES

President George W. Bush signed into law in December 2002 the E-Government Act (Public Law 107-347), which focuses on the need to address the ever-increasing risk of potential security threats to information and information systems in federal agencies. Title III of the Act, entitled the "Federal Information Security Management Act of 2002," requires that all federal agencies provide security for the information and information systems that support the operations and assets of the agency, including those managed by other agencies or contractors.

Based on Federal Information Security Management Act requirements, the National Institute of Standards and Technology developed two types of information security publications: Federal Information Processing Standards and Special Publications (800-series guidance). These publications provide security standards and guidelines that support an enterprisewide risk management process and are an integral part of an agency's overall information security program. The Federal Information Security Management Act and Office of Management and Budget policy[1] require federal agencies to comply with National Institute of Standards and Technology publications. All of the National Institute of Standards and Technology publications anticipate a certain level of system owner involvement in the information security of major applications, prescribing specific roles and responsibilities.

The Federal Information Security Management Act requires HUD to develop, document, and implement an agencywide information security program to ensure that the information systems are protected. This requirement also pertains to any other agencies and contractors whose information systems support HUD's operations. HUD is required to report regularly to the White House, Congress, and Government Accountability Office on the adequacy and effectiveness of information security policies, procedures, and practices that have been implemented. The Federal Information Security Management Act also requires agencies to implement processes to measure information technology security progress and submit quarterly and annual reports to the Office of Management and Budget and Congress, stating progress in areas such as securing information systems and resolving information technology security audit findings. Without a well-designed program, responsibilities may be unclear, misunderstood, and improperly implemented and security controls may be inadequate and inconsistently applied.

HUD relies extensively on information technology to carry out its operations. It is necessary for HUD to develop a departmentwide information security program to protect the availability, integrity and confidentiality of information. HUD's chief information security officer reports directly to the chief information officer and has been assigned the responsibility to direct the management of HUD's information security program. While the Office of Information Technology Security issues and provides oversight to the implementation of departmentwide information security policies and procedures under the direction of the chief information officer and chief information security officer, HUD program offices and system owners are responsible for ensuring appropriate management, operational, and technical controls are effective in protecting the information and information systems under their purview.

[1] The Office of Management and Budget's 2005 Federal Information Security Management Act reporting guidance.

The objective of our audit was to assess HUD’s entitywide information security program compliance with Federal Information Security Management Act requirements. We evaluated 1) the adequacy of categorization of HUD major systems, 2) whether the HUD chief information officer has developed security policies and implemented and monitored enterprisewide security controls, and 3) whether HUD program officials and system owners have properly implemented information security responsibilities assigned to them. We performed this audit as a component of our fiscal year 2005 consolidated financial statement audit and our annual evaluation of HUD’s information security program in the context of the Federal Information Security Management Act.

RESULTS OF AUDIT

Finding 1: HUD's Program Offices and System Owners Incorrectly Classified the Security Level of Its Systems

HUD's application systems and utilities are not properly categorized in accordance with Federal Information Processing Standards Publication 199[2] and National Institute of Standards and Technology Special Publication 800-60[3] due to incomplete implementation of federal guidance. As a result, HUD could have implemented greater security controls than needed and is incurring unnecessary expenditures.

HUD Did Not Accurately Categorize the Security Level of its Information Systems Which Is Critical for Appropriate and Cost-Effective Implementation of Security Controls

Current federal requirements mandate that system owners categorize their information and information systems. The categorization of information systems is critically important as it

- Requires prioritization of information systems according to potential impact on mission or business operations,
- Promotes effective allocation of limited information security resources according to the greatest need,
- Facilitates effective application of security controls to achieve adequate information security, and
- Establishes appropriate expectations for information system protection.

Federal Information Processing Standard Publication 199 provides a standardized approach for establishing security categories for an organization's information and information systems. The security categories are based on the potential impact on an organization should certain events occur, which jeopardize the information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization by operating an information system. This Publication defines three levels of potential impact (low, moderate, or high) on organizations or individuals should there be a breach of security (a loss of confidentiality, integrity, or availability).

[2] "Standards for Security Categorization of Federal Information and Information Systems," dated February 2004.
[3] "Guide for Mapping Types of Information and Information Systems to Security Categories," dated June 2004.

National Institute of Standards and Technology Special Publication 800-60 is posted in two volumes and was written to assist organizations in making the appropriate selection of security controls for their information systems. Volume I provides guidelines for identifying impact levels by type and suggests impact levels for administrative and support information common to multiple agencies. Volume II includes a rationale for information type and impact level recommendations and examples of recommendations for agency-specific mission-related information.

HUD's Overstatement of Security Level Impact For 30 Percent of Its Major Applications May Result in Unnecessary Expenditure of More Than $9.98 Million on Information Security

In our review of HUD's inventory of automated systems, we noted that system owners consistently overstated the security impact level of their applications. Based on guidelines from National Institute of Standards and Technology Special Publication 800-60, HUD inaccurately rated 53 out of 171 major applications. Our analysis indicated that HUD assigned a high security impact level rating for 36 systems for which guidelines recommended a moderate level. We also found that a high security impact level rating was assigned for 17 systems for which guidelines recommended a low level. Using HUD's security control cost estimating tool, we determined that these misclassifications could result in up to $9.98 million in unnecessary annual recurring expenditures. Without a complete review and recategorization, HUD will use these overstated security categorizations in implementing Federal Information Processing Standards Publication 201,[4] which requires greater security measures for high security impact level systems and would require additional funds. The results of our analysis are as follows.

Correct classification	**Number of major applications misclassified as high**	**Additional cost per application****	**Additional annual recurring costs**
Moderate	36	$166,000	$5,832,000
Low	17	$244,000	$4,148,000
Totals	**53***		**$9,980,000**

* 53 out of 171 major applications, representing 31 percent of HUD's major applications.

** Amounts derived by taking the difference between the cost of security for a system classified at the high level and the moderate or low level.

[4] "Federal Information Processing Standards Publication Personal Identity Verification (PIV) of Federal Employees and Contractors," dated February 2005.

Due to a lack of training and awareness of their information security responsibilities, the program offices did not use National Institute of Standards and Technology Special Publication 800-60 guidelines in categorizing their systems. While program officials correctly used federal information processing standards classification terminology, they did not determine security categorizations consistent with National Institute of Standards and Technology guidance. Also, the Office of the Chief Information Officer should have taken a greater role in instructing and guiding the program offices in their system security categorization decisions.

Conclusion

The program offices and system owners have incorrectly categorized a significant number of their major applications, which could cause HUD to incur $9.98 million more than necessary for information security. The program offices and system owners need to evaluate their security level impact consistent with National Institute of Standards and Technology guidance. The Office of the Chief Information Officer needs to provide additional leadership, training, and guidance in the proper categorization of HUD's information and information systems.

Recommendation

We recommend that the Office of the Chief Information Officer

1A. Establish a HUD-wide process to review and categorize information and information systems in accordance with Federal Information Processing Standards and National Institute of Standards and Technology Special Publication 800-60.

1B. Request that the Deputy Secretary require that HUD program offices and system owners categorize their information systems in accordance with the Federal Information Processing Standards Publications and the National Institute of Standards and Technology Special Publication 800-60 so that the additional annual recurring cost of $9.98 million resulting from misclassification will be put to better use.

Finding 2: HUD Has Not Implemented an Entitywide Information Security Program That Fully Complies With Federal Information Security Requirements

HUD has not fully implemented an entitywide information security program in accordance with the Federal Information Security Management Act, Office of Management and Budget Circular A-130, Appendix III[5], and HUD information security management procedures. While the Federal Information Security Management Act Section 3544(b) requires the chief information officer to develop and maintain an agencywide information security program, Section 3544(a) of the Act and HUD's security policy holds program offices and system owners responsible for the successful operation of information technology systems within their program area, and ultimately accountable for the security of the systems and programs under their control. We found that the Office of the Chief Information Officer has not (1) maintained a complete inventory list of information systems; (2) fully complied with federal information security requirements during its accreditation and certification process for major applications and general support systems; (3) established interconnection agreements before connecting their information technology systems to other systems; (4) developed contingency plans for HUD major applications and general support systems; (5) conducted full-scale contingency testing of the plans for high risk-systems to ensure continuity of important functions; and (6) monitored specialized training received by contractor staffs.

The chief information officer and chief information security officer were appointed in fiscal year 2005. Under new leadership, HUD has demonstrated a greater awareness and commitment to improving information security and made significant efforts to improve its system security program during fiscal year 2005. However, HUD has not completely resolved the information security noncompliance issues related to the documentation, implementation, and monitoring of its information program. HUD indicated that it expects to continue working toward fuller compliance in fiscal year 2006. Until HUD completes implementing and maintaining an effective entitywide security program, the confidentiality, availability, and integrity of sensitive information entrusted to HUD could be at risk.

HUD's Inventory of Automated Systems is Not Accurate

HUD's program offices and system owners did not provide the Office of Chief Information Officer a complete list of the information systems maintained by contractors and/or field offices on their behalf. The Federal Information Security Management Act, section 3544(b) requires HUD to develop, document, and implement an agencywide information security program to provide information security for the information and information system that supports the operations

[5] "Management of Federal Information Resources," dated November 2000.

and assets of the agency, including those provided or managed by another agency, contractor, or other source. Also, Office of Management and Budget Circular A-130 requires the head of each agency to maintain an inventory of major systems. HUD's Office of the Chief Information Officer has not developed sufficient procedures for the maintenance of information and information system inventory. As a result, program officials and system owners do not have detailed guidance to assist them in generating and providing an accurate system inventory. While HUD has revised and implemented departmentwide information security policies in fiscal year 2005, detailed information security procedures are not completed. A complete system inventory is the fundamental requirements as it provides the Office of the Chief Information Officer basic information it needs to effectively monitor HUD's entitywide information security program.

HUD's Certification and Accreditation Process Did Not Fully Comply With Federal Information Security Requirements

During our review of HUD's certification and accreditation process for major applications and general support systems, we found that program offices and system owners have not ensured their information systems were in full compliance with federal and the Department's information security requirements. Our review revealed the following weaknesses:

- Major application security documents were not always completed or updated by the application system owners before security documents were submitted to the certification agent for evaluation. As a result, major application information security documents were not updated to reflect changes in applications in a timely manner. For example, none of the 50 major application security plans and risk assessments reviewed reflected the change in location of HUD's data centers or change in risk profile that resulted in the hardware platforms operating system software ownership shifting from HUD to a contractor as part of HUD's new infrastructure contract.
- HUD program offices and system owners did not ensure that testing and evaluations of technical security controls and techniques were conducted periodically to ensure effective implementation of application security controls. Program offices and system owners completed the certification and accreditation of their major applications without testing the adequacy of their technical security controls. In fiscal year 2005, no evaluation of the technical security controls of major applications were performed.

Also, in OIG Audit memorandum DP-06-0801, "OIG Response to Questions from the Office of Management and Budget under the Federal Information System Management Act of 2002," we reported that HUD's system owners have not corrected all of the significant information security vulnerabilities found in the fiscal year 2005 certification and accreditation project. Instead, the program offices and system owners accepted the vulnerabilities to keep their information systems in operation. HUD management stated that HUD has documented the identified security vulnerabilities and asked program offices and system owners to specify in the plans of action and milestone documents the anticipated completion date.

Federal Information Security Management Act Section 3544(b)(5) requires HUD's program offices and system owners make certain that testing and evaluations of technical security controls and techniques are conducted periodically to ensure effective implementation of application security controls. HUD Handbook 2400.25, Section 2.9 states that the program offices and system owners shall i) ensure systems under their purview are certified and accredited; and ii) prepare information system security plan and risk assessments for systems under their purview. Also, HUD Handbook 2400.25, Section 3.1 states that program offices and system owners shall maintain an active and effective system security plan by reviewing and updating system security plans, if needed, once a year.

HUD program offices' and system owners' noncompliance with federal information security requirements may be due to their lack of specialized training regarding their specific information security roles and responsibilities. While current HUD policy holds them ultimately accountable for the security of their program information and information systems, HUD's information security policy and procedures are relatively new. HUD's information technology policy handbook (HUD Handbook 2400.25) was revised during fiscal year 2005. Additionally, HUD issued information technology procedures in September of 2005. However, HUD has not yet fully designed or implemented a role-based information technology security training program that would provide its system owners the training needed to understand and perform all required information security responsibilities. Without adequate security controls at the application level, HUD does not have assurance that it is protected from the unauthorized access, use, modification, or destruction of its information and information systems.

HUD Has Not Consistently Established Systems Interconnection Agreements

Our review of HUD's security plans found that program offices did not always comply with the requirement to document service interconnection agreements when their information was shared internally or externally with other organizations. Office of Management and Budget Circular A-130, Appendix III, Section A.3.a.2(g), requires that government organizations obtain written management authorizations for system interconnection before connecting with other systems. The written authorizations should define rules of behavior and controls that must be maintained for the system interconnection. National Institute of Standards and Technology Special Publication 800-47[6], provides guidance for establishing, maintaining, and terminating interconnections between information systems that are owned and operated by different organizations, including organizations within the same federal agencies. The program offices did not comply with this requirement because the Office of the Chief Information Officer has not developed policies and procedures that provide guidance for documenting agreements governing the interconnections and terms under which the parties will abide by the agreements. Without a well-designed and documented service interconnection agreement, HUD's program offices and system owners are at risk that security failures could compromise the connected systems and the data that they store, process, or transmit.

HUD Has Not Developed Contingency Plans for All Systems and Conducted Full and Complete Testing of Contingency Plans

HUD has not developed contingency plans for all major applications and general support systems listed on the application inventory. HUD expected to develop contingency plans for all of its major applications by December 31, 2005; however, this has not occurred. Appendix III of Office of Management and Budget Circular A-130 requires major applications to have contingency plans that document how managers will perform their mission and/or recover from the loss of existing application support. Additionally, HUD has not performed full-scale testing of contingency plans for all systems with a high security impact level. This testing should include actual relocation to the alternate site and/or system cutover. Instead, HUD performed only table top contingency plan testing for 40 out of 154 systems during fiscal year 2005. The tabletop testing was designed to test the program offices' knowledge and awareness to ensure that participants are aware of their roles. However, the test was limited to questions, answers, and discussion and did not include any hands-on use of equipment that is used during an actual recovery. It did not include a walk-through of the alternate relocation site. HUD's information technology security policy requires that for systems rated with high security impact, the program office and/or system owners shall ensure the performance of testing at the alternate processing site.

[6] "Security Guide for Interconnecting Information Systems," dated August 2002.

HUD Did Not Ensure That Contractor Staff Received Specialized Information Security Training

HUD did not ensure that contractor staff with specialized information security responsibilities received specialized information security training, including HUD-specific information security policy training. Appendix III of Office of Management and Budget Circular A-130, requires that individuals who access high-risk applications receive specialized training focusing on their responsibilities. OMB's fiscal year 2005 instructions for preparing the Federal Information Security Management Act Report and Privacy Management Report states that agencies are fully responsible and accountable for ensuring all FISMA and related policies are implemented and reviewed by contractors and such requirements are included in the terms of the contract, specifically, the agency is responsible for ensuring that contractor personnel receive appropriate training (i.e., general and specific). To date, HUD has not included in its information technology infrastructure contract the ability to monitor the level of security training for contractors with specialized security responsibilities. Contractors who have not received adequate security training and/or are unaware of their security responsibilities may not be properly equipped to effectively perform their assigned duties and increase the risk of causing or allowing a computer security incident to escalate, causing unnecessary harm and damage.

Conclusion

HUD has not completely implemented its information security program and is, therefore, not in compliance with requirements related to the

- Inventory of applications owned by HUD or its contractors or operated by others on HUD's behalf,
- Design and implementation of role-based training for HUD's program offices and system owners,
- Development and implementation of policies and procedures for systems requiring certification and accreditation and HUD's interconnected systems, and
- Implementation plans and procedures for continuity of operations of all systems.

Without implementing and maintaining an effective entitywide security program, the confidentiality, availability, and integrity of sensitive information entrusted to HUD could be at risk.

Recommendations

We recommend that the Office of the Chief Information Officer

2A. Develop and implement procedures for maintaining a complete inventory of information systems owned by HUD or its contractors or operated by others on HUD's behalf.

2B. Design and implement a role-based specialized security training program for program office staff, system owners, and other HUD staff with significant security responsibilities.

2C. Develop system interconnectivity policies that will ensure HUD information is adequately protected from unauthorized access, use, disclosure, disruption, modification, or destruction.

2D. Develop contingency plans for all major applications and general support systems to meet Office of Management and Budget requirements and ensure program offices and system owners implement HUD's information technology security policies by conducting tests at alternate processing sites and documenting the results.

We recommend that the Office of the Chief Information Officer request that the Deputy Secretary direct program officials to

2E. Ensure that information system owners participate in a role-based training program that provides the information security training needed to ensure information system compliance with federal and HUD requirements.

2F. Participate in the development, updating and implementation of security documents and projects for systems under their purview.

2G. Complete implementation of information security protections related to vulnerabilities identified in plans of action and milestone documents.

2H. Establish and maintain service interconnection agreements for information systems supporting the program office mission that are owned and operated by different organizations, including organizations within HUD.

2I. Include federal information security requirements in its information technology infrastructure contracts, specifically, the ability to monitor the specialized training received by contractor staff with significant security responsibilities.

SCOPE AND METHODOLOGY

We performed the audit

- From July through November 2005,
- At HUD Headquarters, Washington, DC, and
- In accordance with generally accepted government auditing standards.

We reviewed HUD’s entitywide information security program, major applications, and general support systems compliance with federal and HUD information security requirements. We focused on security controls, policies, and procedures that were established and implemented during fiscal year 2005.

We performed a detailed security review for 10 systems from HUD’s system inventory list. For each system, we reviewed and analyzed key documents in the certification and accreditation packages and compliance of other security controls required by the Office of Management and Budget, Federal Information Security Management Act, and National Institute of Standards and Technology guidelines. We selected our sample based on the importance to HUD’s mission and as a followup on the status of some critical financial systems that were reviewed in Office of Inspector General (OIG) Audit Report No. 2005-DP-0007, “Review of HUD’s Information System Certification and Accreditation Process.”

To accomplish our objectives, we reviewed policies and procedures, interviewed HUD employees, and obtained and analyzed supporting documentation. We evaluated HUD’s current security program by reviewing the most recent plan of action and milestones documentation for completeness and progress in correcting deficiencies reported in the documents. In addition, we assessed HUD’s process for defining critical systems and evaluated HUD’s general and specialized security training programs for employees and contractors. We also reviewed HUD’s assessment activities for applications, security incident program, and general support systems.

INTERNAL CONTROLS

Internal control is an integral component of an organization's management that provides reasonable assurance that the following objectives are being achieved:

- Effectiveness and efficiency of operations,
- Reliability of financial reporting, and
- Compliance with applicable laws and regulations.

Internal controls relate to management's plans, methods, and procedures used to meet its mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance.

Relevant Internal Controls

We determined the following internal controls were relevant to our audit objectives:

- Policies, procedures, and security controls used for implementing an effective agencywide security program.
- We assessed the relevant controls identified above.

A significant weakness exists if management controls do not provide reasonable assurance that the process for planning, organizing, directing, and controlling program operations will meet the organization's objectives.

Significant Weaknesses

Based on our review, we believe the following items are significant weaknesses:

- HUD's program officials and system owners did not properly categorize the security level of its information systems in accordance with federal requirements, which could cause HUD to incur unnecessary expenditures for information security.
- HUD has not fully implemented an effective agencywide security program to ensure minimum security controls are in place for all systems that are owned by HUD and connected systems owned by other organizations.
- The program officials and system owners have not properly implemented information security responsibilities assigned to them, which prevents their systems from being fully compliant with HUD information security.

APPENDIXES

Appendix A

SCHEDULE OF QUESTIONED COSTS AND FUNDS TO BE PUT TO BETTER USE

Recommendation number	Ineligible 1/	Unsupported 2/	Unreasonable or unnecessary 3/	Funds to be put to better use 4/
1B				$9,980,000

1/ Ineligible costs are costs charged to a HUD-financed or HUD-insured program or activity that the auditor believes are not allowable by law; contract; or federal, state, or local polices or regulations.

2/ Unsupported costs are those costs charged to a HUD-financed or HUD-insured program or activity when we cannot determine eligibility at the time of audit. Unsupported costs require a decision by HUD program officials. This decision, in addition to obtaining supporting documentation, might involve a legal interpretation or clarification of departmental policies and procedures.

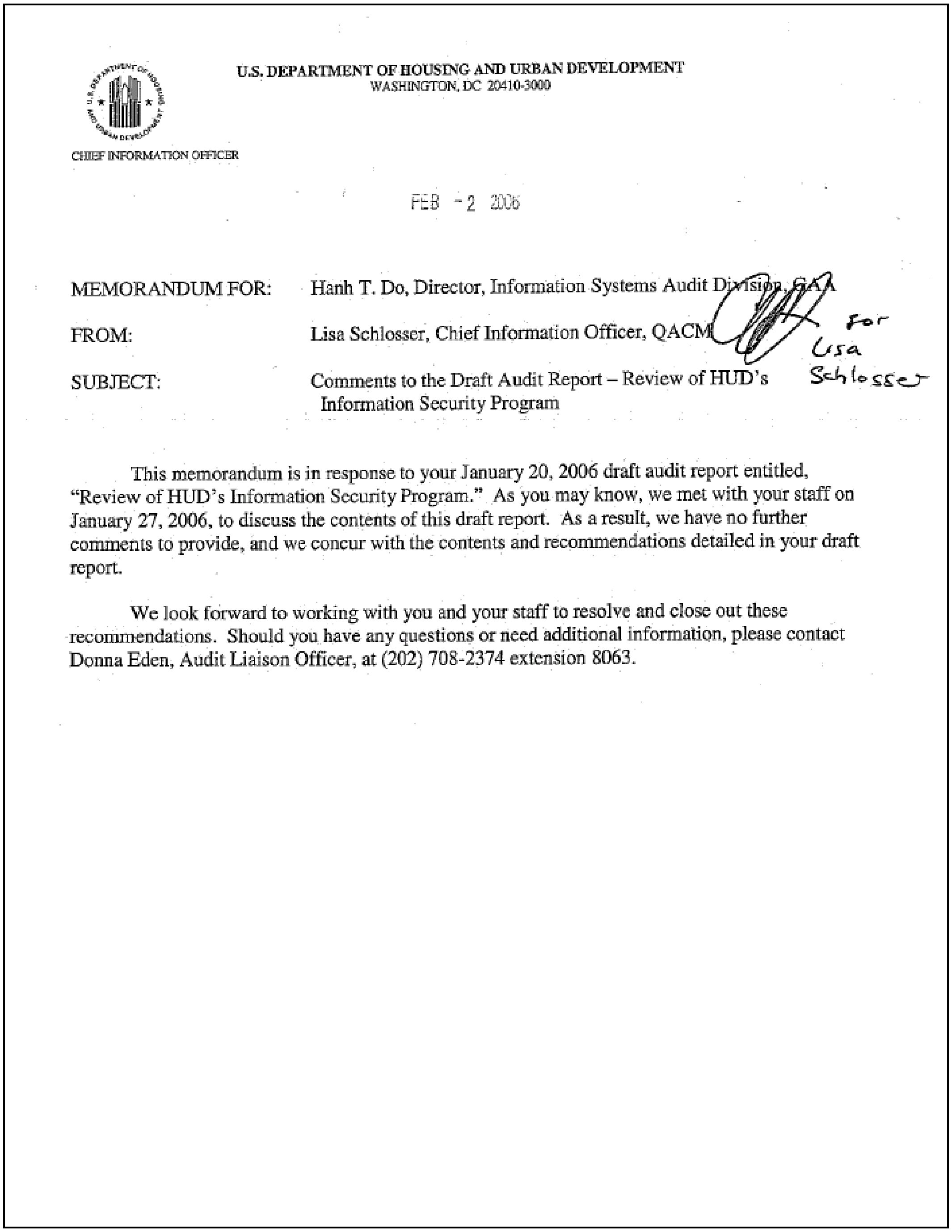
3/ Unreasonable/unnecessary costs are those costs not generally recognized as ordinary, prudent, relevant, and/or necessary within established practices. Unreasonable costs exceed the costs that would be incurred by a prudent person in conducting a competitive business.

4/ "Funds to be put to better use" are quantifiable savings that are anticipated to occur if an OIG recommendation is implemented, resulting in reduced expenditures at a later time for the activities in question. This includes costs not incurred, deobligation of funds, withdrawal of interest, reductions in outlays, avoidance of unnecessary expenditures, loans and guarantees not made, and other savings.

Appendix B

AUDITEE COMMENTS AND OIG'S EVALUATION

<u>Ref to OIG Evaluation</u> **<u>Auditee Comments</u>**



U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
WASHINGTON, DC 20410-3000

CHIEF INFORMATION OFFICER

FEB - 2 2006

MEMORANDUM FOR: Hanh T. Do, Director, Information Systems Audit Division, GAA

FROM: Lisa Schlosser, Chief Information Officer, QACM

For Lisa Schlosser

SUBJECT: Comments to the Draft Audit Report – Review of HUD's Information Security Program

Comment 1

This memorandum is in response to your January 20, 2006 draft audit report entitled, "Review of HUD's Information Security Program." As you may know, we met with your staff on January 27, 2006, to discuss the contents of this draft report. As a result, we have no further comments to provide, and we concur with the contents and recommendations detailed in your draft report.

We look forward to working with you and your staff to resolve and close out these recommendations. Should you have any questions or need additional information, please contact Donna Eden, Audit Liaison Officer, at (202) 708-2374 extension 8063.

OIG Evaluation of Auditee Comments

Comment 1 The Office of the Chief Information Officer concurs with the contents and recommendations detailed in the report.