audit report

Issue Date
April 5, 2007

Audit Report Number
2007-DP-0005

TO: Lisa Schlosser, Chief Information Officer, Q

FROM: Hanh Do, Director, Information Systems Audit Division, GAA

SUBJECT: Review of HUD's Information Technology Security Program

HIGHLIGHTS

What We Audited and Why

We audited the U.S. Department of Housing and Urban Development's (HUD) information security program's compliance with federal requirements. We evaluated (1) the adequacy of the categorization of HUD major systems, (2) whether HUD program officials and system owners have properly implemented their assigned information security responsibilities, and (3) whether HUD's Office of the Chief Information Officer has developed security policies and implemented and monitored enterprise-wide controls. We performed this audit because it is a required component of our fiscal year 2006 consolidated financial statements audit and our annual evaluation of HUD's information system security program in accordance with the Federal Information Security Management Act (FISMA).

What We Found

HUD has continued its progress in implementing a comprehensive, entity-wide set of information system security program policies and procedures. However, several matters require management attention: (1) HUD's program offices and system owners are not performing their FISMA roles and responsibilities related to the updating of security documentation, obtaining role-based training, and testing their applications' technical security controls; and (2) HUD's Office of the Chief Information Officer has not yet fully implemented an effective, entity-wide information security program.

What We Recommend

We recommend that the Office of the Chief Information Officer request that the Deputy Secretary direct program officials to properly perform their information security responsibilities by (1) updating security documents to comply with federal requirements, and (2) continuing the efforts to properly categorize systems they manage and oversee.

We recommend that the Office of the Chief Information Officer fully implement an effective information security program by (1) developing office-specific guidance and procedures as necessary, (2) obtaining training in line with their information security roles and responsibilities, (3) completing the role-based training program for staff with significant security information technology responsibilities, (4) completing the resolution of the current open security vulnerabilities on the general support systems, and (5) providing resources and guidance needed for program offices and system owners to perform technical security control testing on their high-impact applications.

We applaud current efforts of the Chief Information Officer in working with the Office of the Inspector General in addressing program offices compliance with security requirements.

For each recommendation without a management decision, please respond and provide status reports in accordance with HUD Handbook 2000.06, REV-3. Please furnish us copies of any correspondence or directives issued because of the audit.

Auditee's Response

The complete text of the auditee's response, along with our evaluation of that response, can be found in appendix A of this report.

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" (FISMA), 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 FISMA 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). 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 U.S. Department of Housing and Urban Development (HUD) relies extensively on information technology to carry out its operations. It is necessary for HUD's department-wide 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 the Chief Information Officer issues and provides oversight to the implementation of department-wide information security policies and procedures, HUD program offices and system owners are responsible for ensuring that appropriate management, operational, and technical controls are effective in protecting their information and information systems.

The objective of our audit was to assess HUD's entity-wide information security program compliance with FISMA requirements. We evaluated (1) the adequacy of categorization of HUD's major systems, (2) whether HUD program officials and system owners have properly implemented information security responsibilities assigned to them, and (3) whether the HUD Chief Information Officer has developed security policies and implemented and monitored enterprise-wide security controls. We performed this audit as a component of our fiscal year 2006 consolidated financial statement audit and our annual evaluation of HUD's information security program within the context of FISMA.

RESULTS OF AUDIT

Finding 1: HUD's Program Offices and System Owners Are Not in Compliance with Current Information Security Requirements

HUD's program offices and system owners have not completed the implementation of basic security controls over their information systems and data. Specifically, (1) HUD did not update its information systems security documentation, (2) program offices did not test the system-specific technical security controls for their systems, (3) known information security vulnerabilities remain unresolved, and (4) HUD did not correctly identify or categorize all of its information systems. These conditions occurred because HUD's program offices and system owners believe that responsibility for information security belongs to the Chief Information Officer and have indicated that they have not been trained or do not have the needed resources to perform these duties. As a result, HUD cannot adequately ensure that its activities are performed with adequate security or security commensurate with risk, including the potential for harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information as required by law.

HUD Did Not Update Its Information Systems Security Documentation

Not all HUD's program offices[1] and system owners have developed or updated their security planning documents[2] as required by National Institute of Standards and Technology Special Publication 800-53[3]and "HUD Information Technology Security Procedures."[4] They require that security documents for applications be reviewed annually and be revised to address system and organization changes and problems identified during plan implementation or security control assessments. Our review of the application security documents for five program offices found deficiencies in the following areas:

- Four program offices and system owners did not update their security plans to reflect fundamental changes, such as the change in location of the HUD data center and computer platforms on which the applications reside.

[1] HUD program offices referenced in this finding are: the Offices of Administration, Chief Financial Officer, Community Planning and Development, Housing, and Public and Indian Housing/Real Estate Assessment Center.

[2] Security planning documents required by federal guidance include a business impact analysis, risk analysis, and security plan.

[3] "Recommended Security Controls for Federal Information Systems."

[4] "HUD Information Technology Security Procedures," Version 1.4, dated June 9, 2006.

- Four program offices and system owners have risk assessments with incomplete sections or that need to be updated to consider risks associated with the new network infrastructure under the HUD information technology services contracts.
- Three program offices and system owners have application systems that do not have business impact analyses and have developed contingency plans without having conducted business impact analyses.

The program offices and system owners have indicated that the Office of the Chief Information Officer did not provide specialized training and guidance in a timely manner. As a result, they were unsure of how to develop and update the security documents and were waiting for updated training templates. The Office of the Chief Information Officer provided contingency planning training and published system security plan and risk assessment templates at the end of fiscal year 2006. Plans for training system owners on system security plans are being developed. In addition, program office staff noted that there is inadequate funding in their budgets for performing security tasks; i.e., obtaining contractor support for performing risk assessments, updating security plans, and testing technical security controls. With incomplete and outdated security documents, system owners cannot be assured that there are adequate security controls in place for their applications and that they can continue to operate their applications in the event of a disaster.

HUD Program Offices Did Not Test the System-Specific Technical Security Controls for Their Systems

All program offices and system owners have not test all system-specific technical security controls of their applications. FISMA requires testing and evaluation of the security controls in an information system at least yearly. Testing of the common technical controls[5] of HUD applications was performed by the HUD information technology services contractors when they conducted technical control testing on the general support systems.[6] While HUD program offices and system owners can rely on the testing of HUD's general support systems for the technical security controls for their moderate- and low-impact systems, they need to conduct testing of technical security controls that are specific to their high-impact applications.

[5] Results from the assessment of the control that can be used to support the security certification and accreditation processes of another agency information system in which that control has been applied.

[6] Controls that can be applied to one or more agency information systems or an interconnected set of information resources under the same direct management control that share common functionality. It normally includes hardware, software, information, data, applications, communications, and people.

This condition occurred because HUD program offices and system owners were not aware of their information security responsibilities and believe the Office of the Chief Information Officer is responsible for all technical security testing. For example, not all program offices' staff and contractors with specialized security responsibilities attended the specialized training provided by the Office of the Chief Information Officer. Also, the Office of the Chief Information Security Officer does not have the in-house tools or support needed to assist program owners in testing the technical information security controls. Without testing all system-specific information security controls, program offices and system owners are not able to assess the overall security status of a system and the ultimate risk to HUD operations.

Known Information Security Vulnerabilities Remain Unresolved

All five program offices and system owners listed below had a significant number of open information security vulnerabilities and/or delayed actions to correct those vulnerabilities listed in their plans of action and milestones.[7] In their fiscal year 2007 first quarter plans of action and milestones report, four of the program offices and system owners had a high percentage of open vulnerabilities in their systems, for which the corrected actions have been delayed, with no explanation of the reason for the delay. In addition, there are no targeted corrective resolution dates for the open vulnerabilities categorized as delayed as illustrated in the following table.

Program office	Systems operated	Weaknesses (ongoing)	Weaknesses (delayed)	Total	Percentage delayed
Housing	40	108	664	772	86%
Administration	15	48	314	362	87%
Public and Indian Housing/Real Estate Assessment Center	15	52	165	221	86%
Chief Financial Officer	11	0	10	10	100%
Community Planning and Development	3	0	30	30	100%

The plans of action and milestones for the five program offices did not provide a source or estimate of the resources needed to correct the

[7] Generally referred to as "POA&M," this document identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

deficiencies. Office of Management and Budget guidance[8] states that information security plans of action and milestones should provide estimated funding resources required to resolve the weakness as well as the anticipated source of funding; i.e., within the system or as a part of a cross-cutting security infrastructure program. Reporting requirements should include whether a reallocation of base resources or a request for new funding is anticipated. Additionally, HUD program offices and system owners did not include in the plan of action and milestones a column required by the guidance that identifies other, nonfunding obstacles and challenges to resolving the weakness; e.g., lack of personnel or expertise, development of a new system to replace an insecure legacy system, etc., which was not included in documents reviewed.

These open vulnerabilities reflect information security controls that have not been implemented or that have defects in how they were implemented. Until these vulnerabilities are corrected, particularly the "high" and "moderate" vulnerabilities, HUD does not have adequate assurance that the information on the related applications is protected against the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

HUD Did Not Correctly Identify or Categorize All of Its Information Systems

As reported in previous years, HUD continues to over categorize some of its major applications. FISMA tasked the National Institute of Standards and Technology (NIST) with responsibilities for developing standards to assist federal agencies in properly categorizing their information and information systems. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization resulting from the operation of its information systems and the level and types of protection needed. Of HUD's 92 major applications reported in the fiscal year 2006 FISMA report, 31, or 34 percent, were categorized as high impact. This categorization needs to be reassessed, using a data field analysis, based on the following federal guidelines.

- Federal Information Processing Standards (FIPS) Publication 199[9] indicates that impact levels should only be assessed at high when there is an expected severe or catastrophic adverse effect on organization operations, operational assets, or individuals.

[8] Office of Management and Budget Circular M-02-01, "Guidance for Preparing and Submitting Security Plans of Action and Milestones."

[9] "Standards for Security Categorization of Federal Information and Information Systems."

- NIST Special Publication 800-60[10] provides that information systems related to resource allocation, budget formulation, budget execution, asset management, program evaluation, and program monitoring are typically categorized as “low” impact. Systems types that have a “moderate” impact baseline include: continuity of operations, contingency planning, service recovery, financial reporting, accounting, payments, and receivables. Mission information related to homeownership promotion, community development, direct loans, loan guarantees, and general insurance to have a baseline impact level assumption as “low.”
- NIST Special Publication 800-53[11] provides that if a system owner believes that certain additional controls are needed for a higher level of protection, then the system owner can tailor their security control baseline and implementation. For example, if the program office determines that based on their assessment of risk, additional controls are needed to adequately protect the integrity of its software and information then they need to implement the software and information (SI-7)[12] control instead of over categorizing the system.

While HUD policy does refer to FIPS Publication 199 and provides lecture type training, there are insufficient procedures provided to guide program offices and system owners in categorizing systems in HUD’s environment.

Below is a table of selected HUD program offices, the number of systems they own, how many of those are high-impact systems, and the percentage of the program office systems that are categorized as high impact as of January 2007.

[10] “Guide for Mapping Types of Information and Information Systems to Security Categories”

[11] NIST Special Publication 800-53 states that the use of security controls and the incorporation of tailored baseline controls as a starting point in the control selection process facilitates a more consistent level of security across federal information systems. It also offers the needed flexibility to appropriately modify the controls based on specific organizational policy and requirements, particular conditions and circumstances, known threat and vulnerability information, and tolerance for risk to the organization’s operations, assets, or to individuals.

[12] SI-7 Software and information integrity ensures that the information system detects and individuals protects against unauthorized changes to software and information.

Program office	**Systems operated**	**Number of high-impact system**	**Percentage of total**
Administration	14[13]	5	36%
Chief Financial Officer	11	7	64%
Community Planning and Development	3	2	67%
Public and Indian Housing/Real Estate Assessment Center	15	5	36%

The following are examples of systems that need to be reassessed as they may be inappropriately categorized as "high."

- Office of Administration: Facilities Integrated Resource Management System; Grants Interface Management System; Merit Staffing Control System; HUD Integrated Human Resources and Training System; and Enterprise Electronic Records Management/Correspondence Tracking System
- Office of the Chief Financial Officer: Section 235 Automated Validating and Editing; Line of Credit Control System (LOCCS) HUD's Centralized Accounting and Program System (HUDCAPS); Administrative Accounting-Personal Services Cost Report Subsystem; Financial Data Mart, Program Accounting System; and Bondmapper
- Office of Community Planning and Development: Integrated Disbursement and Information System; and Special Needs Assistance Program
- Public and Indian Housing/Real Estate Assessment Center: Voucher Management System; Financial Assessment Sub-System; Tenant Eligibility Assessment Sub-system; Physical Assessment Sub-System-PIH/REAC; and PIH Inventory Management System

Systems that are over categorized would require additional security expenditures and significantly more testing of controls. HUD has used a budget tool in the past, which indicates that a high-impact system costs $700,000 more per system than a low-impact system.

As of January 17, 2007, HUD also appears to have incorrectly identified two major applications as minor applications. They are the Loan Accounting System and the HUD Consolidated Financial Statement System. As HUD considered them to be minor applications, the system

[13] Our review noted a discrepancy between the fiscal year 2006 FISMA report, January 19, 2006, system inventory, and the fiscal year 2007 first quarter plans of action and milestones. We will follow up on HUD's current processes for maintaining an accurate inventory of systems during our fiscal year 2007 FISMA work.

owners were not required to perform the required self-assessment or update the security documentation.

Conclusion

HUD program offices' and system owners' lack of compliance with current information security requirements, due to a lack of understanding on their roles and responsibilities related to information security, may compromise their ability to ensure that information systems and data are adequately protected.

Recommendations

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

1A. Ensure that all major application security documentation is made current and is in full compliance with current federal requirements.

1B. Review the authority to operate any major application with known information security vulnerabilities that are in a delayed status with no stated date for resolution and ensure that application plans of action and milestones comply with reporting requirements in Office of Management and Budget Circular M02-01, "Guidance for Preparing and Submitting Security Plans of Action and Milestones."

We recommend that the Office of the Chief Information Officer

1C. Develop department-wide guidance and procedures for the testing of system-specific technical controls on all major applications.

1D. Provide detailed training classes to assist program offices and system owners in properly categorizing their systems using a data field analysis method.

Finding 2: HUD's Chief Information Officer Has Not Fully Implemented an Entity-Wide Information Security Program That Fully Complies with Federal Information Security Requirements

HUD's Chief Information Officer has not completed the implementation of an effective, entity-wide security program. Areas that still require management attention include (1) continuing efforts to implement a comprehensive role-based training program for HUD staff with significant information security responsibilities, (2) conducting a complete set of tests on high-impact systems, and (3) resolving open information system security vulnerabilities for general support systems. While HUD's Chief Information Officer continues working toward fuller compliance in fiscal year 2006, HUD's policies and procedures related to the condition noted were not fully developed and implemented at the time of our review due to a lack of resources. Without a well-designed, entity-wide security program, there is an increased risk that responsibilities are unclear, misunderstood, and improperly implemented; and security controls are inadequate and inconsistently applied.

HUD Has Not Developed and Implemented a Comprehensive Role-Based Training and Security Awareness Training Program

HUD has neither completed the design and implementation of a role-based training program for program office staff and contractors with significant information security responsibilities. HUD's Office of the Chief Information Officer held a series of lectures on information security issues for contractors and HUD program offices' staff, including system owners and security administrators. The lectures included discussions on information technology contingency planning, conducting business impact analyses, FISMA requirements, National Institute of Standards and Technology publications, and federal information processing standards. While the coverage of these topics was necessary and useful, the depth of coverage and engagement of HUD employees and contractors is not sufficient to provide them the comprehensive understanding of their roles and responsibilities needed to ensure that their applications are adequately protected. Also, staff within the program offices, such as information system owners, office coordinators, and system administrators, often either do not receive adequate role-based information security training or receive the training in an untimely manner. As a result, security documents are outdated, and system security categorization efforts are inadequate.

The federal information security manager handbook[14] states that role-based training should provide security courses that are tailored to the specific needs of each group of people who have been identified as having significant responsibilities for information security in their organization.

HUD information technology policies and procedures do not (1) provide adequate guidance to all staff with significant information technology responsibilities (e.g., office information technology coordinators and system owners) and (2) address role-based training for program office staff and system owners. HUD indicated that it is in the process of updating its procedures, including updating the roles and responsibilities of HUD staff.

Current federal guidance[15]on information technology security training refers to the security basics and literacy category as a transitional stage between awareness and training, providing the foundation for additional training by providing a universal baseline of key security terms and concepts. After "security basics and literacy," federal guidance requires training to be focused on providing the knowledge, skills, and abilities specific to an individual's roles and responsibilities relative to information technology systems. For example, system owners should receive training in the acceptance of residue risks as part of the certification and accreditation process, and system administrators should be aware of audit trail and encryption requirements. At this level, an information security training program needs to consider the differences between beginning, intermediate, and advanced skill requirements. Most of HUD information security training deficiencies reside at the beginning and intermediate skill levels. The next level, which is advanced, relates to education and experience and focuses on developing the ability and vision to perform complex multidisciplinary activities. With adequate security training, HUD can ensure that trained, professional staff supports the Chief Information Security Officer.

Without requiring program office staff who have significant security roles to take appropriate information security training, HUD's program offices information will continue to be at risk.

[14] NIST Special Publication 800-100, "Information Security Handbook: A Guide for Managers."

[15] NIST Special Publication 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model."

HUD Did Not Resolve Known Information Security Vulnerabilities Found in General Support Systems

We reported in an Office of Inspector General (OIG) audit[16] that as of third quarter fiscal year 2006, HUD's outsourced general support systems have a number of known information security vulnerabilities that are classified as delayed with no stated date for resolution. In our review of HUD's information security fiscal year 2007 first quarter plans of action and milestones for HUD's general support systems, operated by Lockheed Martin and Electronic Data Systems (EDS), we noted that HUD continues to have "open" and "delayed" information security vulnerabilities in the following categories.

General support system	**High risk**		**Moderate risk**		**Low risk**		**Total open vulnerabilities**
	Delayed	**Ongoing**	**Delayed**	**Ongoing**	**Delayed**	**Ongoing**	
IBM mainframe	2	0	9	0	3	0	14
Internet server	0	0	2	0	3	0	5
LAN* file server	1	0	23	0	9	1	34
Intranet server	0	0	10	0	0	0	10
Lotus Notes	1	0	13	0	6	0	20
Unisys mainframe	1	0	11	0	5	0	17
WAN**	1	0	1	2	0	3	7
Totals	**6**	**0**	**69**	**2**	**26**	**4**	**107**

* Local area network
** Wide area network

Most of these vulnerabilities have remained open since the fall of 2005 when they were identified as part of the certification and accreditation process. HUD's Chief Information Security Officer signed the certification statement for Lockheed Martin- and EDS-operated general support systems with the understanding and belief that all high-risk vulnerabilities would be fixed according to existing remediation plans. Additionally, HUD anticipated that Lockheed Martin and EDS would continue to correct the deficiencies with moderate- and low-risk information security controls. However, there was no estimated completion date indicated in the information security plan of action and milestones for the open vulnerabilities classified as delayed.

HUD has not established an effective process for reporting discovered information security vulnerabilities in its plan of action and milestones. In more than a year of operating HUD's general support systems, neither EDS nor Lockheed Martin identified and reported any information

[16] OIG Audit Report No. 2007-DP-0002, "Review of HUD's Information Technology Services (HITS) Contracts," dated January 18, 2007.

security vulnerability to HUD that was included on the plan of action and milestones. According to requirements in Office of Management and Budget Circular A-130, EDS and Lockheed Martin should have regularly tested and evaluated information security controls, which should have identified weaknesses in the management, operational, or technical information security controls for their general support systems to be included on the plan of action and milestones report, as required by FISMA.

The significance of information security vulnerabilities on general support systems is that they degrade the protections needed by the applications which reside on them. These vulnerabilities reflect information security controls that have not been implemented or that have defects in how they were implemented. Without the resolution of these vulnerabilities, particularly the "high" and "moderate" vulnerabilities, none of HUD's applications have adequate assurance of protection against the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

HUD Has Not Implemented Adequate Testing of Common Technical Controls for Its High-Impact Systems

HUD has not conducted the complete set of tests on its high-impact information systems' common security controls as required by FISMA. The tests of technical controls were not performed as part of HUD's fiscal years 2004 and 2005 certification projects, which was a defect in the process. The lack of testing significantly impacts only the high-impact systems, as HUD did conduct technical control tests on all of its general support systems at the moderate-impact level in fiscal year 2005 and HUD's moderate- and low-impact systems can use the testing as support. HUD security management informed us that system owners are responsible for testing their applications that need information system controls above the common controls tested under the general support system moderate-level baseline requirements. However, in the intervening years, HUD has not acquired the tools or contractor support or developed guidance to assist system owners in performing those tests on its high-impact systems.

FISMA and Office of Management and Budget Circular A-130 both require the annual review of controls. Program office management has accepted the risk of operating these systems without a complete understanding of what security vulnerabilities exist for the systems. Since the systems in question are categorized as high impact, it can be assumed that HUD would suffer a catastrophic loss if the information in these systems is compromised or the application unable to function.

Without the adequate testing of these high-impact technical controls, the program owners cannot provide themselves with adequate assurance that the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the agency.

Conclusion

Because HUD has not yet completed the implementation of its current set of information security policies and procedures; its information technology security program has not fully addressed all of the HUD-specific information security issues necessary to ensure a fully compliant program.

Recommendations

We recommend that the Office of the Chief Information Officer

2A. Develop and implement a role-based training program for program office system owners and other staff with information technology security responsibilities.

2B. Resolve the open information security vulnerabilities contained in the plan of action and milestones documents for HUD general support systems operated by the HITS[17] contractors.

2C. Obtain the resources and develop guidance necessary for program offices and system owners to be able to perform the required testing of technical information security controls on their high-impact applications.

[17] HUD Information Technology Services (HITS) refers to HUD’s outsourced information technology infrastructure contracts.

SCOPE AND METHODOLOGY

We performed the audit

- From February 2006 through January 2007,
- At HUD headquarters, Washington, DC, and
- In accordance with generally accepted government auditing standards.

We reviewed HUD's entity-wide 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 2006.

We used a random statistical sampling method to evaluate the compliance of HUD program offices and system owners in maintaining and updating security documents for the systems under their purview. Using statistical sampling software, we randomly selected 42 major applications from the universe of 108 HUD major applications reported in HUD's system inventory list as of June 2006.[18] The 42 major applications are managed by five HUD program offices: the Offices of Administration, Chief Financial Officer, Community Planning and Development, Housing, and Public and Indian Housing/Real Estate Assessment Center. 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, FISMA, and National Institute of Standards and Technology guidelines. Additionally, we reviewed the status of the information security controls on the general support systems on which these applications are operated.

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, the security incident program, and general support systems.

[18] HUD reported 92 systems in its October 2006 Annual FISMA Report to the Office of Management and Budget (OMB), which is the number used later in this report. The reason for the difference between the 108 systems in our sample selection and the 92 systems reported to OMB is that HUD program offices have since reviewed major and minor systems' identification and changed a number of them.

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, agency-wide 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:

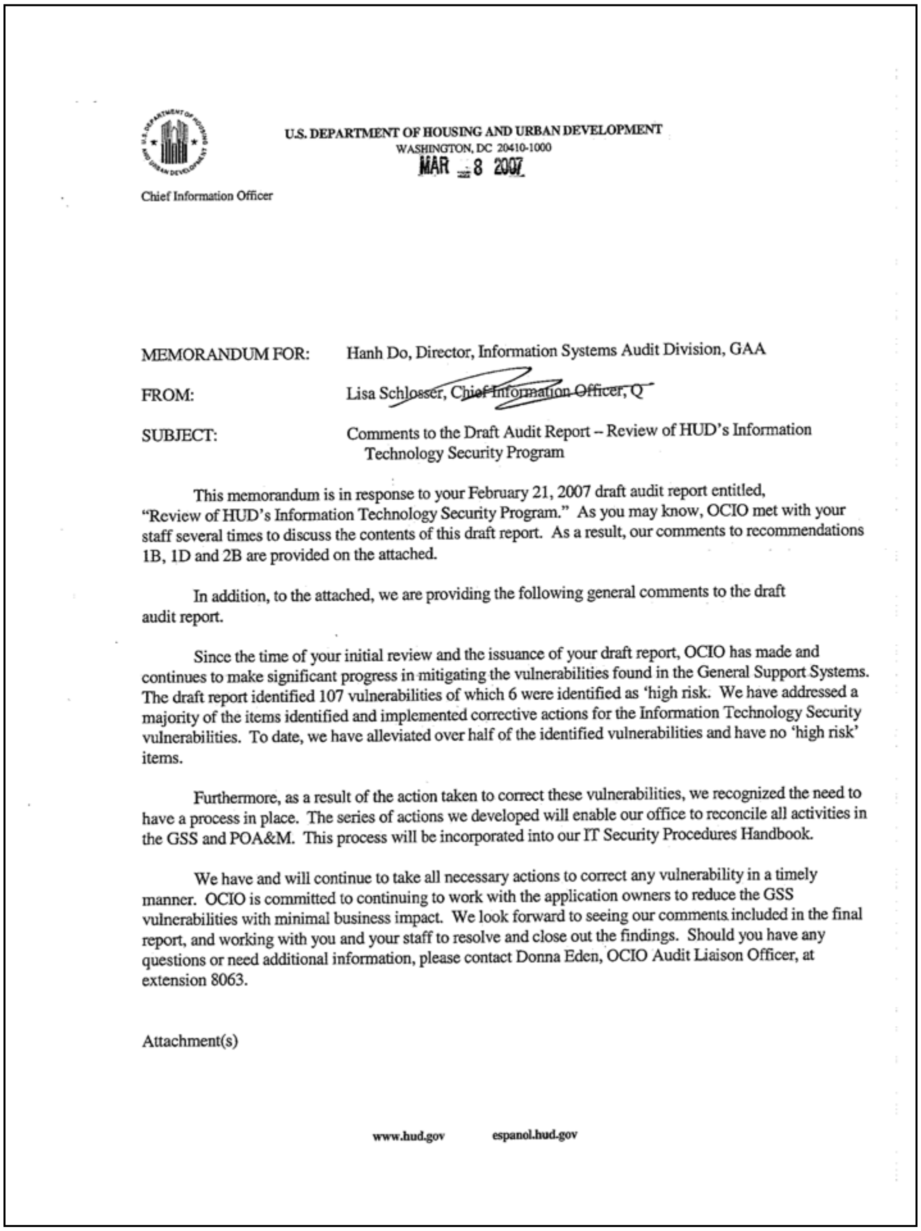
- The program officials and system owners have not properly implemented information security responsibilities assigned to them, which prevents their systems from being fully compliant with HUD information security requirements (finding 1).
- HUD has not fully implemented an effective, agency-wide security program to ensure that minimum security controls are in place (finding 2).

APPENDIXES

Appendix A

AUDITEE COMMENTS AND OIG'S EVALUATION

Ref to OIG Evaluation **Auditee Comments**



U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
WASHINGTON, DC 20410-1000
MAR 8 2007

Chief Information Officer

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

FROM: Lisa Schlosser, Chief Information Officer, Q

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

This memorandum is in response to your February 21, 2007 draft audit report entitled, "Review of HUD's Information Technology Security Program." As you may know, OCIO met with your staff several times to discuss the contents of this draft report. As a result, our comments to recommendations 1B, 1D and 2B are provided on the attached.

In addition, to the attached, we are providing the following general comments to the draft audit report.

Comment 1

Since the time of your initial review and the issuance of your draft report, OCIO has made and continues to make significant progress in mitigating the vulnerabilities found in the General Support Systems. The draft report identified 107 vulnerabilities of which 6 were identified as 'high risk. We have addressed a majority of the items identified and implemented corrective actions for the Information Technology Security vulnerabilities. To date, we have alleviated over half of the identified vulnerabilities and have no 'high risk' items.

Furthermore, as a result of the action taken to correct these vulnerabilities, we recognized the need to have a process in place. The series of actions we developed will enable our office to reconcile all activities in the GSS and POA&M. This process will be incorporated into our IT Security Procedures Handbook.

We have and will continue to take all necessary actions to correct any vulnerability in a timely manner. OCIO is committed to continuing to work with the application owners to reduce the GSS vulnerabilities with minimal business impact. We look forward to seeing our comments included in the final report, and working with you and your staff to resolve and close out the findings. Should you have any questions or need additional information, please contact Donna Eden, OCIO Audit Liaison Officer, at extension 8063.

Attachment(s)

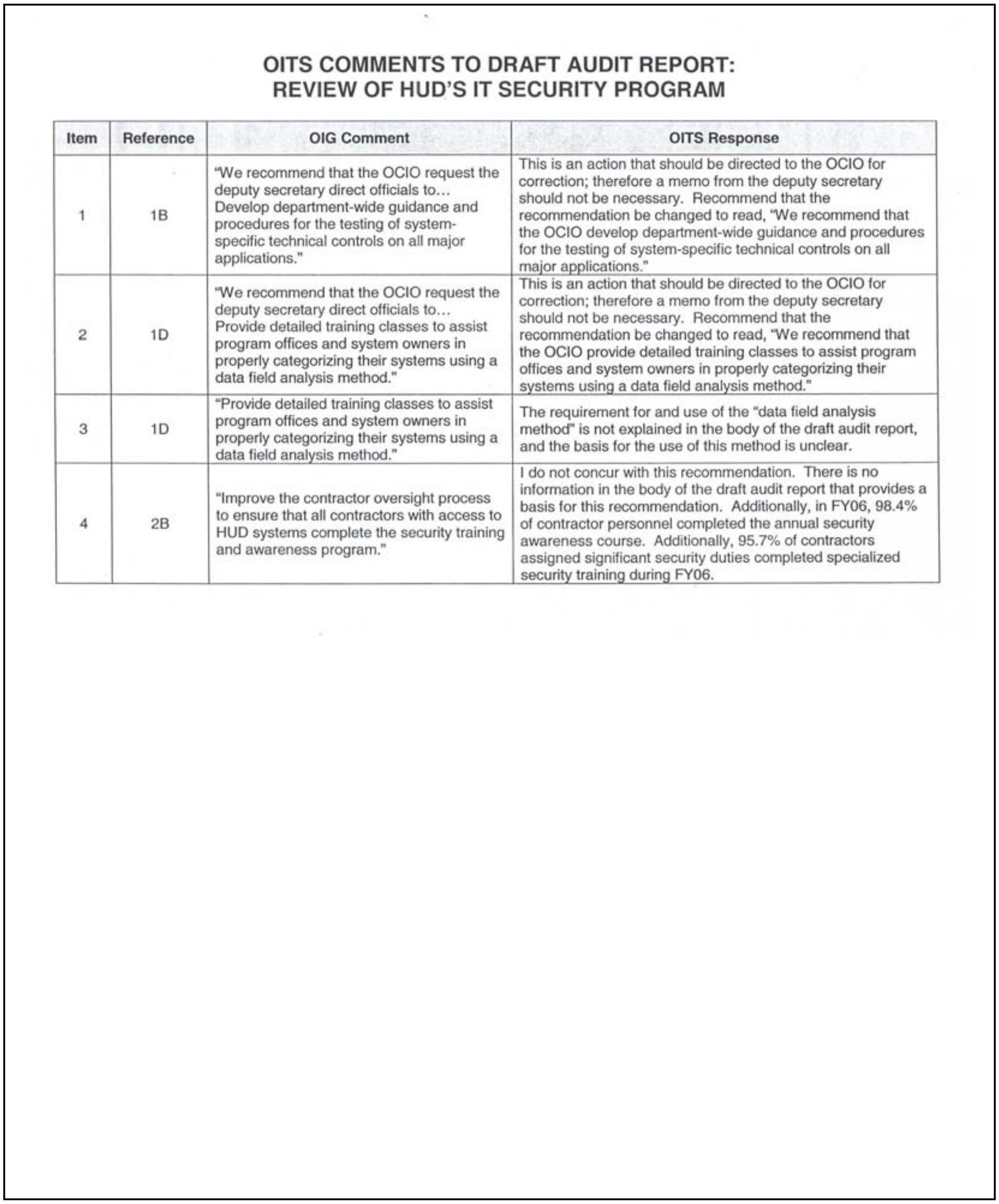
www.hud.gov espanol.hud.gov

Comment 2

Comment 3

Comment 4

Comment 5



OITS COMMENTS TO DRAFT AUDIT REPORT: REVIEW OF HUD'S IT SECURITY PROGRAM

Item	Reference	OIG Comment	OITS Response
1	1B	"We recommend that the OCIO request the deputy secretary direct officials to… Develop department-wide guidance and procedures for the testing of system-specific technical controls on all major applications."	This is an action that should be directed to the OCIO for correction; therefore a memo from the deputy secretary should not be necessary. Recommend that the recommendation be changed to read, "We recommend that the OCIO develop department-wide guidance and procedures for the testing of system-specific technical controls on all major applications."
2	1D	"We recommend that the OCIO request the deputy secretary direct officials to… Provide detailed training classes to assist program offices and system owners in properly categorizing their systems using a data field analysis method."	This is an action that should be directed to the OCIO for correction; therefore a memo from the deputy secretary should not be necessary. Recommend that the recommendation be changed to read, "We recommend that the OCIO provide detailed training classes to assist program offices and system owners in properly categorizing their systems using a data field analysis method."
3	1D	"Provide detailed training classes to assist program offices and system owners in properly categorizing their systems using a data field analysis method."	The requirement for and use of the "data field analysis method" is not explained in the body of the draft audit report, and the basis for the use of this method is unclear.
4	2B	"Improve the contractor oversight process to ensure that all contractors with access to HUD systems complete the security training and awareness program."	I do not concur with this recommendation. There is no information in the body of the draft audit report that provides a basis for this recommendation. Additionally, in FY06, 98.4% of contractor personnel completed the annual security awareness course. Additionally, 95.7% of contractors assigned significant security duties completed specialized security training during FY06.

OIG Evaluation of Auditee Comments

Comment 1 As part of our fiscal year 2007 audit work, we plan to verify the information provided by reviewing the management process employed, plans of actions and milestones, updated policies and procedures, and supporting documentation used to close the vulnerabilities.

Comment 2 We agree. We renumbered recommendation 1B to 1C and addressed the recommendation directly to the OCIO.

Comment 3 We agree. We addressed the recommendation directly to the OCIO.

Comment 4 We have added clarifications in the text of the report to refer to a data field analysis.

Comment 5 We have removed the recommendation and supporting text. We plan to review HUD’s updated process for ensuring that all of its contractors receive the appropriate security training, including security awareness training in fiscal year 2007.