



U.S. Department of Housing and Urban Development
Office of Inspector General
451 7th St., S.W.
Washington, D.C. 20410

September 28, 2007

MEMORANDUM NO.: 2007-DP-0801

MEMORANDUM FOR: Bajinder Paul, Acting Chief Information Officer, Q

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

SUBJECT: OIG Response to Questions from the Office of Management and Budget
Under the Federal Information Security Management Act of 2002

Introduction

The Federal Information Security Management Act of 2002 (FISMA) requires the Office of the Inspector General (OIG) to perform an annual independent evaluation of the U.S. Department of Housing and Urban Development's (HUD) information security program and practices. This memorandum presents the results of our evaluation.

Methodology/Scope

This evaluation is based on prior audits, audits in progress, and review of HUD's most recent plans of action and milestones. OIG also analyzed HUD's progress in correcting deficiencies reported in the plans of action and milestones and reported in audit reports.

Background

Office of Management and Budget (OMB) Memorandum M-07-25, "FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," dated July 25, 2007, provides reporting instructions to federal agencies and the inspectors general. The memorandum requests agency inspectors general to respond to specific questions in the format provided. Our responses to the questions are contained in appendix A, a spreadsheet provided by the Office of Management and Budget.

FOR OFFICIAL USE ONLY

Results of Review

1) HUD has taken steps to improve information system security. Specifically, HUD has

- a) Developed and delivered specialized training for program office system owners that covered risk assessment, framework for security planning, and contingency plan testing.
- b) Issued a memorandum to senior program staff from the Deputy Secretary and conducted biweekly meetings with the program information system security officer to ensure that the security policy is properly implemented at the program and system level.
- c) Reviewed and recategorized systems' security impact levels to ensure compliance with Federal Information Processing Standards (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems," and National Institute of Standards and Technology Special Publication (NIST SP) 800-60, "Guide for Mapping Types of Information and Information Systems to Security Categories."
- d) Prepared privacy impact assessments for all major applications and new systems and prepared a template to ensure that assessments prepared for all systems that contain personally identifiable information (PII) are in accordance with OMB Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002."
- e) Developed a new interconnection security agreement template for HUD systems connected to other agencies' systems to ensure that security controls for the interconnections are in place.
- f) Acquired "Watchfire," an application verification and validation tool, which will be used to evaluate HUD Web application programming. The Office of the Chief Information Officer (OCIO) provided the "Watchfire" application security training to program offices in fiscal year 2007.
- g) Initiated a comprehensive review of E-Authentication Risk Assessments (ERA) to ensure the quality of information provided by system owners and full compliance with OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies." This effort has included development of a standard template, revised instructions, provision of ERA training, and development of updated policies and procedures for performing ERAs.

2) HUD needs to take additional actions to be in full compliance with FISMA's security requirements.

- a) HUD's program offices and system owners have not always ensured that HUD's inventory of automated systems is accurate and up-to-date as required by OMB Memorandum A-130. Examples are as follows:

FOR OFFICIAL USE ONLY

- HUD has not disconnected obsolete systems from its network and removed these systems from its inventory of automated systems in a timely manner. The risk of potential security threats to HUD information and information systems is increased because system owners and OCIO have stopped correcting security weaknesses or performing the annual self-assessments for these obsolete systems.
- OIG's Audit Report number 2007-DP-0006, "Review of HUD's Personal Identity Verification and Privacy Program," dated August 28, 2007, noted that system owners did not include a system in HUD's inventory of automated systems even though the system contains PII data.

As a result, HUD cannot be sure that all security requirements have been reviewed and implemented for the systems.

- b) HUD has not properly categorized all systems with PII data. OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," states that agencies should generally consider categorizing systems with PII data as moderate or high. HUD OCIO has taken OIG's advice to inform system owners and program offices to categorize their system with PII as a moderate or high risk impact level. However, we identified systems with PII data that have not been recategorized from low to the moderate or high risk level.
- c) HUD program offices were unable to complete an annual assessment of security controls for major applications and general support systems before OIG's completion of its fiscal year 2007 FISMA review. OMB Memorandum A-130, "Management of Federal Information Resources," requires agencies to perform annual testing and evaluation of the effectiveness of information security policies, procedures, and practices, including the testing of management, operational, and technical controls. HUD officials expect to complete the self-assessments by September 30, 2007; however, this does not provide OIG adequate time to review these self-assessments.

Further, HUD has not tested and evaluated the technical security controls of its major applications categorized as high impact. HUD's OCIO informed system owners during fiscal year 2007 that OCIO would ensure that the common technical controls for all applications categorized as moderate or low were implemented and tested, and system owners would be responsible for the additional controls needed for systems rated high. However, HUD's OCIO has not officially issued department-wide guidance and procedures for the testing of system-specific technical controls on all major applications to the program offices. HUD OCIO officials expect to issue the final policies and procedures by January 2008. By not assessing the security controls against criteria and standards in NIST SP 800-53, "Recommended Security Controls for Federal Information Systems," HUD cannot be assured that the security

FOR OFFICIAL USE ONLY

controls have been implemented correctly and ensure that information is adequately protected.

- d) OCIO has not shared the assessment results of general support systems and technical common controls implemented in general support systems with the information system security officers (ISSO) and the system owners of major applications. NIST SP 800-18, "Guide for Developing Security Plans for Federal Information Systems," requires OCIO to ensure that the required common controls are put into place, the controls are assessed, and the assessment results are shared with the appropriate information system owners. In addition, OCIO does not always share major changes made to general support systems with the ISSOs and system owners. As a result, ISSOs and system owners cannot be certain that all security requirements are in place for their systems and be aware of all risks that might adversely affect their systems.
- e) HUD does not perform annual contingency plan testing for major applications with a low risk impact level. The fiscal year 2007 FISMA instruction requires annual contingency plan testing for systems that are required to be certified and accredited. HUD conducted certification and accreditation for all major applications but did not perform annual contingency plan testing for major applications with a low risk impact level because there is no such requirement in the current NIST SP 800-53. The new requirement was published in the FISMA instruction released on July 25, 2007, and HUD, therefore, has not had time to conduct the testing.
- f) HUD's business impact assessment does not include all elements required by NIST SP 800-34, "Contingency Planning Guide for Information Technology Systems." During our review of business impact assessment for eight systems, we noted that the business impact assessment did not contain the following elements outlined in NIST SP 800-34: system architecture and diagrams, system manager name and contact information, and other internal and external critical user points of contact. These elements are necessary to support the other documents that are generated from the business impact analysis, i.e., the continuity of operations plan and the business resumption plan.
- g) HUD still has many delayed weaknesses with no corrective action plan and new projected completion dates. FISMA, section 3544(b)(6), requires HUD's information security program to include a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in its information security program policies, procedures, and practices. There are weaknesses that have remained open since fiscal year 2003. Deputy Secretary Bernardi issued a memorandum on March 14, 2007, requesting program offices to resolve all information security weaknesses by November 30, 2007, or work with OCIO to establish an acceptable risk acceptance plan.

FOR OFFICIAL USE ONLY

- h) HUD has not conducted annual testing of the incident response capability for outsourced systems. HUD has not implemented the requirement to conduct annual testing of the incident response capability for outsourcing information systems as outlined by NIST SP 800-53 and HUD information technology (IT) policies and procedures.
- i) HUD program offices and system owners did not ensure that their staff with significant IT security roles and responsibilities participated in a role-based IT security training program. NIST SP 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model," requires agencies to ensure that training be given to individuals that matches their specific job duties. During our review of the Federal Housing Administration's (FHA) controls over its information technology resources, FHA's system owners indicated that they did not receive role-based training, and the security administrators did not receive any additional technical training. Also, in Audit Report number 2007-DP-0006, "Review of HUD's Personal Identity Verification and Privacy Program," dated August 28, 2007, OIG reported that system owners and the officials responsible for the security of two systems with PII in the Office of Security & Emergency Planning (OSEP) did not attend specialized training related to information security requirements. Program officials and system owners 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 proliferating a computer security incident.
- j) HUD did not always ensure that system configuration requirements were implemented for its systems. During a review of Unisys performance and security controls, we found that HUD had adopted the Department of Defense's Security Technical Implementation Guide as guidance for implementing baseline technical security controls for HUD's Unisys operating systems. However, HUD did not tailor the security guidelines to reflect its environment and its policies, procedures, and regulations. Further, the security configuration checklist used by a HUD contractor has not been approved, is incomplete, and does not provide detailed guidelines to implement HUD's policy and procedures in regard to Unisys operating systems. In addition, in Audit Report number 2007-DP-0007, "Vulnerability Assessment of HUD's Computer Network," dated September 19, 2007, OIG reported that HUD did not ensure that all known vulnerabilities were patched to HUD computer workstations.
- k) HUD's program office and system owners have not completed all system e-authentication risk assessments. HUD Handbook 2400.25, REV-1, requires program office and system owners to conduct the e-authentication risk assessment of the transactional systems under their purview, following the guidance in OMB Memorandum M-04-04, "E-Authentication Guidance for

FOR OFFICIAL USE ONLY

Federal Agencies.” HUD’s Office of IT Security identified 195 HUD systems that require an e-authentication risk assessment. However, as of September 7, 2007, HUD program offices and system owners had completed e-authentication risk assessments for only 46 systems. As a result, HUD cannot adequately 1) determine its authentication needs for electronic transactions, 2) identify and analyze the risks associated with each step of the authentication process, and 3) ensure that an appropriate level of assurance is provided to all electronic transactions with authentications.

3) HUD’s certification and accreditation process needs to be improved.

- HUD OCIO did not comply with its own certification and accreditation policy in regard to monitoring significant change on general support systems. In fiscal year 2007, HUD made significant changes to the intranet and Internet general support systems as it upgraded the operating system and introduced new hardware into the environment. However, HUD did not perform a security impact assessment on these changes to the two general support systems as required by HUD and federal policies. The purpose of the security impact assessment is to document HUD’s consideration of the changes in security controls and/or additional risk exposure. As this particular operating system was a major upgrade and introduced significant new functionality, HUD should have performed a full test and evaluation of the implemented security controls. Further, HUD did not update the respective general support systems’ security documentation, i.e., business impact assessment, risk assessment, security plan, and contingency plans, to reflect these changes. During OIG’s review of Unisys performance and security controls, we also noted that the security plan for the general support system, Unisys 2200 operating system, is not current.
- HUD has not ensured that all nonmajor applications are covered in the certification and accreditation of a general support system and documented the additional required security controls for minor applications. NIST SP 800-37 requires certification and accreditation for all major applications and allows nonmajor applications to be covered in the certification and accreditation of a general support system or a major application. NIST SP 800-18 requires that the additional controls specific to the minor application be documented in the system security plan as an appendix or paragraph.
- HUD placed systems into production before they were fully certified and accredited. HUD has developed system security plans and conducted risk assessments before some systems were certified and accredited. However, HUD certified and accredited systems before it conducted the independent and comprehensive assessment of management, operational, and technical security controls in the systems, which is required by NIST SP 800-37. Additionally, in Audit Report number 2007-DP-0006, “Review of HUD’s Personal Identity Verification and Privacy Program,” dated August 28, 2007, OIG reported that

FOR OFFICIAL USE ONLY

two systems supporting HUD's personal identity verification process that contains PII data had been in production for several years without certification and accreditation or supporting security documents. Without certification and accreditation of general support and application systems, management cannot be assured that the systems have undergone a complete evaluation of risk or that appropriate mitigating and compensating controls have been put in place.

4) HUD has not fully implemented the following technical controls required by OMB to protect PII:

- HUD has not implemented encryption for laptops. OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," requires agencies to encrypt all data on mobile computers/devices carrying agency data unless the data are determined not to be sensitive. The Deputy Secretary or a senior-level individual may designate this in writing.
- HUD has not implemented the two-factor authentication on all enterprise remote access solutions. OMB Memorandum M-07-16 requires agencies to allow remote access only with two-factor authentication when one of the factors is provided by a device separate from the computer gaining access.
- HUD has not implemented the requirement to log computer-readable data extracts and the destruction of sensitive data. OMB Memorandum M-07-16 requires an agency to log all computer-readable data extracts from databases holding sensitive information and verify each extract, including whether sensitive data have been erased within 90 days or use of the data is still required.
- HUD has not reported every incident involving PII to the United States Computer Emergency Readiness Team within one hour of discovering the incident. OMB requires agencies to report all incidents involving PII in electronic or physical form and not distinguish between suspected and confirmed breaches.

Without implementing appropriate administrative, technical, and physical controls to safeguard PII, HUD cannot ensure the PII data entrusted to HUD are protected from misuse or unauthorized access.

cc:

Walter Harris, Deputy Chief Information Officer, Q
Patrick Howard, Chief Information Security Officer, QACC
Homa Zarrinnahad, Director, Network Services Management, QTB
John W Smith, Computer Specialist, QACC
Wanda Taylor, Audit Liaison, QDAM

FOR OFFICIAL USE ONLY

OIG Responses to OMB Questionnaire

Section C - Inspector General: Questions 1 and 2													
Agency Name: U.S. Department of Housing and Urban Development		Submission date:											
Question 1: FISMA Systems Inventory													
1. As required in FISMA, the IG shall evaluate a representative subset of systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.													
In the table below, identify the number of agency and contractor information systems, and the number reviewed, by component/bureau and FIPS 199 system impact level (high, moderate, low, or not categorized). Extend the worksheet onto subsequent pages if necessary to include all Component/Bureaus.													
Agency systems shall include information systems used or operated by an agency. Contractor systems shall include information systems used or operated by a contractor of an agency or other organization on behalf of an agency. The total number of systems shall include both agency systems and contractor systems.													
Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency; therefore, self-reporting by contractors does not meet the requirements of law. Self-reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.													
Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing													
2. For the Total Number of Systems reviewed by Component/Bureau and FIPS System Impact Level in the table for Question 1, identify the number and percentage of systems which have: a current certification and accreditation, security controls tested and reviewed within the past year, and a contingency plan tested in accordance with policy.													
Bureau Name	FIPS 199 System Impact Level	Question 1						Question 2					
		a. Agency Systems		b. Contractor Systems		c. Total Number of Systems (Agency and Contractor systems)		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and reviewed in the past year		c. Number of systems for which contingency plans have been tested in accordance with policy	
		Number	Number Reviewed	Number	Number Reviewed	Total Number	Total Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
ADMIN	High	3				3	0						
	Moderate	6				6	0						
	Low	4	1	1		5	1	1	100%	0	0%	0	0%
	Not Categorized					0	0						
	Sub-total	13	1	1	0	14	1	1	100%	0	0%	0	0%
CFO	High					0	0						
	Moderate	13	1			13	1	1	100%	1	100%	1	100%
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	13	1	0	0	13	1	1	100%	1	100%	1	100%
CPD	High	1	1			1	1	1	100%		0%	1	100%
	Moderate	1				1	0						
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	2	1	0	0	2	1	1	100%	0	0%	1	100%
DEPSEC	High					0	0						
	Moderate	2	1			2	1	1	100%	0	0%	1	100%
	Low	0				0	0						
	Not Categorized					0	0						
	Sub-total	2	1	0	0	2	1	1	100%	0	0%	1	100%
ENFC	High					0	0						
	Moderate	0				0	0						
	Low	1	1	0		1	1	1	100%	0	0%	0	0%
	Not Categorized					0	0						
	Sub-total	1	1	0	0	1	1	1	100%	0	0%	0	0%
FHEO	High					0	0						
	Moderate	2	1			2	1	1	100%	0	0%	1	100%
	Low	1				1	0						
	Not Categorized					0	0						
	Sub-total	3	1	0	0	3	1	1	100%	0	0%	1	100%
GNMA	High					0	0						
	Moderate	0		5	1	5	1	1	100%	0	0%	1	100%
	Low	0		1		1	0						
	Not Categorized					0	0						
	Sub-total	0	0	6	1	6	1	1	100%	0	0%	1	100%
HSG	High					0	0						
	Moderate	29		1		30	0						
	Low	5				5	0						

FOR OFFICIAL USE ONLY

	Not Categorized					0	0						
	Sub-total	34	0	1	0	36	0	0	0	0	0	0	0
OCIO	High			0		0	0						
	Moderate	0		7	1	7	1	1	100%	0	0%	1	100%
	Low	2	1			2	1	1	100%	0	0%	0	0%
	Not Categorized					0	0						
	Sub-total	2	1	7	1	8	2	2	100%	0	0%	1	50%
OIG	High					0	0						
	Moderate	0		1		1	0						
	Low	0				0	0						
	Not Categorized					0	0						
	Sub-total	0	0	1	0	1	0	0		0		0	
PDR	High					0	0						
	Moderate	1	1			1	1	1	100%		0%	1	100%
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	1	1	0	0	1	1	1	100%	0	0%	1	100%
PIH	High					0	0						
	Moderate	3	1			3	1	1	100%	0	0%	1	100%
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	3	1	0	0	3	1	1	100%	0	0%	1	100%
REAC	High	1	1			1	1	1	100%	0	0%	1	100%
	Moderate	5				5	0						
	Low	4				4	0						
	Not Categorized					0	0						
	Sub-total	10	1	0	0	10	1	1	100%	0	0%	1	100%
SEC	High					0	0						
	Moderate	1	1			1	1	1	100%	0	0%	1	100%
	Low	0				0	0						
	Not Categorized					0	0						
	Sub-total	1	1	0	0	1	1	1	100%	0	0%	1	100%
Agency Totals	High	5	2	0	0	6	2	2	100%	0	0%	2	100%
	Moderate	83	8	14	2	77	8	8	100%	1	13%	8	100%
	Low	17	3	2	0	18	3	3	100%	0	0%	0	0%
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Total	85	11	16	2	101	13	13	100%	1	8%	10	77%

FOR OFFICIAL USE ONLY

Section C - Inspector General: Questions 4 and 5																		
Agency Name: U.S. Department of Housing and Urban Development																		
Question 4: Evaluation of Agency Plan of Action and Milestones (POA&M) Process																		
<p>Assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestones (POA&M) process. Evaluate the degree to which each statement reflects the status in your agency by choosing from the responses provided. If appropriate or necessary, include comments in the area provided.</p> <p>For each statement in Items 4.a. through 4.f., select the response category that best reflects the agency's status.</p> <p>Response Categories:</p> <ul style="list-style-type: none"> - Rarely- for example, approximately 0-50% of the time - Sometimes- for example, approximately 51-70% of the time - Frequently- for example, approximately 71-80% of the time - Mostly- for example, approximately 81-95% of the time - Almost Always- for example, approximately 96-100% of the time 																		
4.a.	The POA&M is an agency-wide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency.	Almost Always (96-100% of the time)																
4.b.	When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s).	Mostly (81-95% of the time)																
4.c.	Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly).	Almost Always (96-100% of the time)																
4.d.	Agency CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	Almost Always (96-100% of the time)																
4.e.	IG findings are incorporated into the POA&M process.	Almost Always (96-100% of the time)																
4.f.	POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.	Almost Always (96-100% of the time)																
<p>OIG comments to 4.f: HUD still has many delayed weaknesses with no corrective action plans and projected completion dates. For additional details, see section 2.g of the attached memorandum.</p>																		
Question 5: IG Assessment of the Certification and Accreditation Process																		
<p>Provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Provide narrative comments as appropriate.</p> <p>Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" (May 2004) for certification and accreditation work initiated after May 2004. This includes use of the FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems" (February 2004) to determine a system impact level, as well as associated NIST document used as guidance for completing risk assessments and security plans.</p>																		
5.a.	<p>The IG rates the overall quality of the Agency's certification and accreditation process as:</p> <p>Response Categories:</p> <ul style="list-style-type: none"> - Excellent - Good - Satisfactory - Poor - Failing 	Satisfactory																
5.b.	<p>The IG's quality rating included or considered the following aspects of the C&A process: (check all that apply)</p>	<table border="1" style="width: 100%;"> <tr><td>Security plan</td><td style="text-align: center;">X</td></tr> <tr><td>System impact level</td><td style="text-align: center;">X</td></tr> <tr><td>System test and evaluation</td><td style="text-align: center;">X</td></tr> <tr><td>Security control testing</td><td style="text-align: center;">X</td></tr> <tr><td>Incident handling</td><td style="text-align: center;">X</td></tr> <tr><td>Security awareness training</td><td style="text-align: center;">X</td></tr> <tr><td>Configurations/patching</td><td style="text-align: center;">X</td></tr> <tr><td>Other:</td><td></td></tr> </table>	Security plan	X	System impact level	X	System test and evaluation	X	Security control testing	X	Incident handling	X	Security awareness training	X	Configurations/patching	X	Other:	
Security plan	X																	
System impact level	X																	
System test and evaluation	X																	
Security control testing	X																	
Incident handling	X																	
Security awareness training	X																	
Configurations/patching	X																	
Other:																		
<p>OIG comments to 5.b: HUD has certified and accredited 100 percent of its major applications and general support systems. However, HUD did not perform a full test and evaluation of the implemented security controls when significant changes were made to two general support systems. HUD certified and accredited new systems before they conducted the independent and comprehensive assessment of management, operational and technical security controls in the systems. For additional details, see section 3 of the attached memorandum.</p>																		

FOR OFFICIAL USE ONLY

Section C - Inspector General: Questions 6 and 7		
Agency Name:		
Question 6: IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process		
6.a.	<p>Provide a qualitative assessment of the agency's Privacy Impact Assessment (PIA) process, as discussed in Section D II.4 (SAOP reporting template), including adherence to existing policy, guidance, and standards.</p> <p>Response Categories:</p> <ul style="list-style-type: none"> - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing <p>OIG Comments: HUD has developed policies, procedures and a template to ensure PIA are prepared for all systems contain personally identifiable information (PII) in accordance with OMB memorandum 03-22.</p>	Good
6.b.	<p>Provide a qualitative assessment of the agency's progress to date in implementing the provisions of M-06-15, "Safeguarding Personally Identifiable Information" since the most recent self-review, including the agency's policies and processes, and the administrative, technical, and physical means used to control and protect personally identifiable information (PII).</p> <p>Response Categories:</p> <ul style="list-style-type: none"> - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing <p>OIG Comments: While HUD has updated blackberries configurations to include full encryption for blackberry devices, HUD has not encrypted laptops at this time. For additional details, see section 4 of the attached memorandum.</p>	Satisfactory
Question 7: Configuration Management		
7.a.	<p>Is there an agency-wide security configuration policy? Yes or No.</p> <p>OIG Comments: HUD has not always ensured that the minimally acceptable system configuration requirements are implemented for its systems. See section 2-j of the attached memorandum.</p>	Yes
7.b.	<p>Approximate the extent to which applicable information systems apply common security configurations established by NIST.</p> <p>Response categories:</p> <ul style="list-style-type: none"> - Rarely- for example, approximately 0-50% of the time - Sometimes- for example, approximately 51-70% of the time - Frequently- for example, approximately 71-80% of the time - Mostly- for example, approximately 81-95% of the time - Almost Always- for example, approximately 96-100% of the time 	Almost Always (96-100% of the time)

FOR OFFICIAL USE ONLY

Section C - Inspector General: Questions 8, 9, 10 and 11	
Agency Name:	
Question 8: Incident Reporting	
Indicate whether or not the agency follows documented policies and procedures for reporting incidents internally, to US-CERT, and to law enforcement. If appropriate or necessary, include comments in the area provided below.	
8.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No. Yes
8.b.	The agency follows documented policies and procedures for external reporting to US-CERT. Yes or No. (http://www.us-cert.gov) No
8.c.	The agency follows documented policies and procedures for reporting to law enforcement. Yes or No. Yes
OIG Comments: HUD did not report every incident involving personally identifiable information to US-CERT within one hour of discovering the incident.	
Question 9: Security Awareness Training	
Has the agency ensured security awareness training of all employees, including contractors and those employees with significant IT security responsibilities?	Almost Always (96-100% of employees)
Response Categories: - Rarely- or approximately 0-50% of employees - Sometimes- or approximately 51-70% of employees - Frequently- or approximately 71-80% of employees - Mostly- or approximately 81-95% of employees - Almost Always- or approximately 96-100% of employees	
Question 10: Peer-to-Peer File Sharing	
Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training? Yes or No.	Yes
Question 11: E-Authentication Risk Assessments	
The agency has completed system e-authentication risk assessments. Yes or No.	No
OIG Comments: During our review of FHA controls over its information technology resources, FHA's system owners indicated that they did not receive role-based training, and the security administrators did not receive any additional technical training. For additional details, see section 2-1 of the attached memorandum.	

FOR OFFICIAL USE ONLY

Appendix B

Comments from the U.S. Department of Housing and Urban Development



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

CHIEF INFORMATION OFFICER

SEP 28 2007

MEMORANDUM FOR:

Hanh Do, Director, Information Systems Audit
Division, GAA

FROM:

Walter Harris, Deputy Chief Information Officer, Q

SUBJECT:

Response to the Federal Information Security Management
Act of 2002 (FISMA) Report

This is in response to your memorandum entitled "Response to Questions from OMB under the Federal Information Security Management Act of 2002." My staff has reviewed your memorandum and we are in agreement with the results of your review.

We look forward to working with you and your staff to continue to improve our Information Technology Security Program. Should you have any questions on the matter, please contact Patrick Howard, Office of Information Technology Security at 202-402-8094.