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

MEMORANDUM NO.:
2006-DP-0801

October 4, 2005

MEMORANDUM FOR: Lisa Schlosser, Chief Information Officer, AY

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 System 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 Department of Housing and Urban Development's (HUD) information security program and practices. This memorandum presents the results of our evaluation.

METHODOLOGY AND SCOPE

Our evaluation is based on our prior audits, our audits in progress, and our review of HUD's most recent plan of action and milestones. We also analyzed HUD's progress in correcting deficiencies reported in the plan of action and milestones and reported in audit reports that we have issued.

BACKGROUND

Office of Management and Budget Memorandum M-05-15, "FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," dated June 13, 2005, provides reporting instructions to federal agencies and inspectors general. The memorandum requests agency inspectors general to respond to specific questions in the format provided. Our responses to the questions are contained within Appendix B, a spreadsheet provided by the Office of Management and Budget.

RESULTS OF REVIEW

HUD has made significant efforts to improve its system security program, but continued progress is needed to fully comply with federal requirements. HUD has appointed a chief information security officer, revised its information security policy, and completed certification and accreditation for more than 90 percent of its applications. However, the quality of the underlying documents and the actual certification and accreditation process varied by application. While a number of vulnerabilities were closed, additional vulnerabilities, identified through oversight activities, were not corrected before accreditation. We also found that HUD has not fully implemented required elements of the agencywide information security program as specified in FISMA sections 3544(a) and 3544(b).

1. HUD has taken steps to improve information system security by

a) Appointing a Chief Information Security Officer to head the Office of Information Technology Security;

b) Certifying and accrediting more than 90 percent of its applications;

c) Updating and publishing its entitywide information technology security policy;

d) Completing the transition phase of its information technology infrastructure contract, which included information system security as a core function;

e) Engaging contractor support to assist in entitywide security program enhancements; and

f) Implementing an enterprisewide generalized security awareness training program covering HUD and contractor staff.

2. HUD program officials and system owners have made progress in meeting their information security responsibilities, although some aspects of this responsibility remain to be met as specified in FISMA section 3544(a).

a) The FISMA requirement for maintaining an adequate system inventory has not been fully met. Not all program offices and system owners provided the Office of the Chief Information Officer a listing of information systems maintained on behalf of HUD by contractors or field offices as required by FISMA section 3544(a)(1)(A)(ii). The Federal Housing Administration had applications operated for them by contractors that were not included in HUD's information security monitoring activities. In addition, there are systems that are hosted by HUD's field offices without the knowledge of the chief information security officer, who is, therefore, unable to monitor their information security.

b) Application-level security duties and responsibilities are not always known by program office staff. HUD program officials and information system owners have not fully implemented HUD and other federal information security policies as required by FISMA section 3544 (a)(1)(B). HUD's Office of Information Technology Security assigned all required security responsibilities to system owners in fiscal year 2005 by issuing entitywide information security policies that address current federal information security requirements and outline program officials' and system owners' security responsibilities. However, there have been few training and awareness efforts by HUD's program offices to ensure that their system owners, program managers, and information technology staff and managers are familiar with the new information security policies and their responsibilities.

c) HUD has not fully integrated information security management into its management processes. FISMA section 3544 (a)(1)(C) requires the integration of information security management into strategic and operational planning processes. HUD program offices have not been able to fully comply with this requirement because of the way in which it has historically managed and funded information security. For new applications and projects, HUD manages its capital planning through an information technology investment management process, which involves management and technical and operational reviews by HUD staff of various levels. HUD's Office of the Chief Information Officer, within the last year, revised its System Development Methodology process to include policy compliance with information security requirements, which have not been fully implemented for all HUD information systems.

d) HUD's program offices and system owners need to be more actively involved in the development of security plans and risk assessments. FISMA section 3544 (a)(2)(A) requires that HUD program office and system owners assess the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems. In fiscal year 2005, the Office of the Chief Information Officer attempted to centralize the development of security plans and risk assessments for HUD's applications and general support systems. However, our review of some HUD's program office information security documents found that system owner involvement appeared to be limited. Many of the documents had missing application-specific information, out-of-date contact points, and other gaps and omissions.

e) HUD program offices and system owners may have categorized their security impact at too high a level. FISMA section 3544 (a)(2)(B) requires that HUD program offices determine the level of information security appropriate to protect information and information systems. HUD has issued an information security policy that requires system owners to categorize their systems. For all 251 systems and utilities within HUD's Inventory of Automated Systems, we found

that the systems were categorized using the security category terms[1] as established by the Federal Information Processing Standards 199[2]. However, system owners did not adequately apply National Institute of Standards and Technology Special Publication 800-60[3] guidance for assigning the security impact levels. The systems that the Publication recommends categorizing as high impact are those that provide information technology infrastructure maintenance[4] and information management[5]. Our cursory review of the 70 systems and utilities categorized as high in the inventory found the levels may be overstated based on the Publication's recommendations.

f) HUD could reduce information security costs if the systems are categorized in accordance with National Institute of Standards and Technology guidance. FISMA section 3544 (a)(2)(C) requires HUD to implement policies and procedures to cost-effectively reduce risks to an acceptable level. Misclassification of multiple systems at too high a security level would require HUD to implement a higher level of security controls (and, therefore, may be more costly) than is needed to adequately protect its information and information systems. As indicated above, HUD may have categorized 70 of its systems and utilities at too high a level. In May of 2005, HUD's chief information security officer requested that program offices review their information systems security categorization. Only 47 of 251 (19 percent) applications and utilities were reviewed. The security levels were increased for 9 and decreased for 29, while 9 remained unchanged.

g) HUD has not fully tested and evaluated security controls of all systems. FISMA section 3544 (a)(2)(D) requires program offices and system owners to periodically test and evaluate security controls and techniques to ensure they are effectively implemented. HUD has made efforts to comply with this requirement using a centralized approach. The Office of the Chief Information Officer has regularly had contractor support in performing reviews of its general support systems technical security controls. HUD's seven general support systems are currently being certified and accredited. HUD's chief information security officer has established a deadline of September 30, 2005, for all systems owners to complete the annually required self-assessment. Additionally, HUD expects to complete the certification process of its general support systems in early fiscal year 2006.

[1] Low, moderate, and high – potential impact on an organization should certain events occur, which jeopardize the information and information systems needed by the organization to accomplish its assignment mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.
[2] Standards for Security Categorization of Federal Information and Information Systems, (February 2004).
[3] Guide for Mapping Types of Information and Information Systems to Security Categories.
[4] Supports the planning, design, implementation, and maintenance of an information technology infrastructure to effectively support automated needs.
[5] Supports the coordination of information collection, storage, dissemination, and destruction, as well as managing the policies, guidelines, and standards regarding information management.

h) HUD's chief information security officer has not fully implemented processes to monitor information security on an agencywide basis. FISMA section 3544 (a)(3)(B) requires the development and maintenance of an agencywide information security program. HUD appointed a chief information security officer on May 2, 2005. While possessing appropriate experience and background, and making significant progress on the monitoring the Department's information security vulnerabilities, HUD's chief information security officer lacks the authority and resources to oversee and enforce the security requirements of HUD's information and information systems on an agencywide basis. We noted that the chief information security officer had difficulty obtaining information regarding information security from program offices and independent agencies with applications that do not reside in HUD's infrastructure. For example,

- The Federal Housing Administration did not provide information security information on its property management contractors' systems.

- The Office of Federal Housing Enterprise Oversight was not included in fiscal year 2005 oversight activities as HUD did not consider it a reportable component.

i) HUD's information security policies do not include all required federal requirements. FISMA section 3544 (a)(3)(C) requires HUD's chief information security officer to develop and maintain information security policies, procedures, and control techniques. HUD revised and issued its Information Technology Security Handbook in fiscal year 2005. The Handbook seeks to address all applicable federal information security requirements; assign roles and responsibilities to HUD staff; and serve as a resource for information system owners, program staff, and others involved in securing information and information systems. We noted the following in our review of HUD's information security policy, procedures, and control techniques:

- HUD does not have sufficient procedures that provide for the maintenance of an inventory of all of its information systems that includes systems operated on its behalf by contractors or other organizations.

- HUD has communicated with program and technical staff the requirements for security plans, business impact analysis, and certification and accreditation. However, deficiencies remain in the related documents and executed processes. HUD has not provided adequate training to its system owners and program management on its information security requirements related to

    - Categorization of system information,
    - Risk assessments, and
    - System interconnection agreements

j) HUD has not ensured that all contractor staff with specialized information responsibilities have received specialized security training. FISMA section 3544 (a)(3)(D) requires that HUD provide additional security training and awareness for program office staff with specialized information security responsibilities. While HUD has consistently provided a general annual security training and awareness program for its staff, contractors (who have access to HUD's intranet), and the Office of the Chief Information Officer's Office of Information Technology staff, it does not ensure that contractors, having special security-related responsibilities and operating information systems for HUD, receive required security training. For example, HUD did not include in its information technology infrastructure contract the ability to monitor the level of security training for staff with specialized security responsibilities.

3. HUD has not fully implemented an agencywide information system security program as specified in FISMA section 3544(b). While HUD has made progress in fiscal year 2005, certain information security program components are not fully compliant.

a) Our review of 50 (out of 152) risk assessments performed found them to be inadequate. FISMA section 3544(b)(1) of the Act requires that HUD's information security program conduct periodic assessments of risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. HUD has established a policy that requires periodic assessments of risks and reviews these assessments as part of its information security program. Federal guidance requires that issues identified in these reviews be used to update security plan and risk assessment documents. Adequate risk assessment and security plan helps to identify appropriate controls for reducing or eliminating risk. We found deficiencies in all 50 risk assessments and 10 security plans we reviewed. Security plans were developed and risk assessments were conducted for applications and utilities without sufficient security reviews, program office participation, and assessments of risk.

b) HUD's information security program has not completed implementation of all required policies and procedures needed to fully comply with federal requirements. FISMA section 3544(b)(2) requires that HUD's information security program have promulgated policies and procedures that are based on risk assessments and that are cost effective in reducing information security risks and ensure that information security is addressed throughout the information system lifecycle. The chief information security officer has conducted reviews of the primary HUD infrastructure sites for compliance with federal requirements. While HUD has implemented department wide information security policies in fiscal year 2005, HUD's detailed information security procedures are not yet complete.

While HUD has made progress in developing configuration policy and guidance, it has not fully implemented the security configuration requirements in accordance with FISMA section 3544(b)(2)(D)(iii) for all of its applications and database management software. In our audit report 2005-DP-0005, "Security of Windows 2000 Server," we found that HUD has generally implemented the Microsoft Windows 2000 operating system configuration settings properly. However, deficiencies in configuration security and backup and recovery practices were identified. We also found that

- HUD does not ensure compliance for connections to nonagency systems in accordance with National Institute of Standards and Technology Special Publication 800-47, "Security Guide for Interconnecting Information Technology Systems" (August, 2002).

- Contingency plans have not been fully documented, and provisions for disaster recovery process testing have not been arranged for HUD's non-mission-critical applications. Twenty-three contingency plans of HUD's 41 mission-critical systems have been tested during fiscal year 2005.

c) HUD's information security program does not provide security training and awareness to all contractor staff with access to HUD's systems. FISMA section 3544(b)(4) requires that HUD provide security awareness training to personnel, including contractors and other users of information systems, of the risks associated with their activities and their responsibilities in complying with HUD's policies and procedures designed to reduce those risks. HUD's Office of the Chief Information Officer does not have a comprehensive training program for contractors performing these functions. The chief information security officer is aware of this requirement and has overseen the current training program, which has provided generalized security training to 95 percent of HUD staff and specialized training to 99 percent of HUD staff with significant security responsibilities. The chief information security officer plans to implement an expanded training program to incorporate contractor staff when possible. Within the current training program, 72 percent of contractor staff received the generalized security training during fiscal year 2005.

d) HUD has not fully designed or implemented periodic tests and evaluations of the effectiveness of information security policies, procedures, and practices for its major applications. FISMA section 3544(b)(5) requires that HUD perform periodic tests and evaluations of the effectiveness of information security policies, procedures, and practices. These tests should include testing of management, operational, and technical controls of every information system in the inventory. HUD's Office of the Chief Information Security Officer stated that in fiscal year 2005, HUD's work on the certification and accreditation process' software test and evaluation and related work covered the material and met the requirement. However, HUD has not performed reviews and assessments of major applications which tested the effectiveness of assessments of all information security technical

controls. HUD's Office of Information Technology Security has asked HUD program offices to review and revise, as necessary, their information security self-evaluation checklists and submit them for review prior to September 30, 2005. However, it is unlikely that the program offices would be able to properly assess their technical information security controls.

e) HUD's information system vulnerabilities planned action and milestones process is used to manage known corrective actions. 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. The Office of the Chief Information Officer implemented and maintains the plan of action and milestones database for applications, utilities, and general support systems. The program offices prioritize and update the database based on planned corrective actions. The database is then used as the basis for quarterly reporting to the Office of Management and Budget. This process was followed for all of fiscal year 2005.

f) HUD's information security program policies and procedures for security incidents were not followed by a HUD component. FISMA section 3544(b)(7) requires that HUD's information security program include procedures for detecting, reporting, and responding to security incidents. HUD has implemented high-level policy on security incidents and the reporting of security incidents. However, department wide procedures were not adequately communicated. For example, the Office of Federal Housing Enterprises, an independent agency within HUD, had a security incident in fiscal year 2005 but did not report the incident to the Office of the Chief Information Officer because it was not aware of the policy and procedures. Our review of HUD's security training and awareness program found discussion of threats and vulnerabilities but no guidance to users on reporting security incidents to the Office of the Chief Information Officer. HUD has recently obtained additional contractor support to assist with monitoring the infrastructure contractor and to perform its own tests and analysis.

g) HUD's information security program has not fully implemented an adequate contingency planning process for the development and testing of the plans. FISMA section 3544(b)(8) requires that HUD's information security program include plans and procedures to ensure continuity of operations for information systems that support HUD's operations and assets. HUD has only recently begun to train program offices and system owners of their responsibilities to prepare contingency plans for their information systems. Based on our review of 10 of HUD's major information systems, HUD system owners have not consistently developed, maintained, or tested, business continuity plans, business recovery plans, disaster recovery plans, continuity of support plans, or cyber incident response plans.

4) **Overall quality of HUD's certification and accreditation process**

In fiscal year 2005, HUD certified and accredited its major applications and is making significant progress on its general support systems. As of August 31, 2005, HUD has certified more than 90 percent of its major applications. However, the quality of the underlying documents and the actual process varied by application. There were many vulnerabilities that were not corrected before accreditation. In our audit report 2005-DP-0007, "Review of HUD's Information Systems Certification and Accreditation Process," we found that the quality of the process for certification and accreditation of HUD information systems in calendar year 2004 was poor, resulting in incomplete certification and accreditation packages.

Acknowledging deficiencies in the process, HUD hired a contractor to perform a qualitative analysis of the fiscal year 2004 certification and accreditation activities on each HUD application. The contractor reviewed implemented security controls, software test and evaluation results documents, security plans, risk assessments, and contingency plans. This analysis resulted in the identification of numerous additional information security vulnerabilities, which were documented in the application's planned action and milestone documents. HUD was then able to certify the applications. Application owners, after reviewing the information security vulnerabilities and accepting the risks, signed the certification letter. As of August 31, 2005, HUD has not corrected all of the identified vulnerabilities.

HUD has not completed the certification and accreditation of its seven general support systems. However, the process is underway, and progress is being made. HUD has completed initial scans on all general support systems. It has completed a plan of action and milestones document that identified vulnerabilities, which are in the process of being addressed. The chief information security officer indicated that the intranet general support system (which supports the Federal Housing Administration financial systems) is expected to be accredited in November 2005 and the remaining general support systems will be accredited in early fiscal year 2006.

Comments from the Department of Housing and Urban Development

U. S. Department of Housing and Urban Development
Washington, D.C. 20410-3000

September 30, 2005

CHIEF INFORMATION OFFICER

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

FROM: Lisa Schlosser, Chief Information Officer, AY

SUBJECT: Response to the Federal Information Systems Management Act of 2002 (FISMA) Report

This is in response to your September 27, 2005, draft memorandum entitled, "OIG Response to Questions from OMB under the Federal Information System Management Act of 2002." My staff has reviewed your draft 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 this matter, please contact Donna Eden, Director, Office of Policy and E-Government at 202-708-0614 ext. 8063.

Appendix B

Section C: Inspector General. Questions 1, 2, 3, 4, and 5.

Agency Name: U.S. Department of Housing and Urban Development

Question 1 and 2

1. As required in FISMA, the IG shall evaluate a representative subset of systems, including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of systems reviewed in this evaluation for each classification below (a., b., and c.).

To meet the requirement for conducting a NIST Special Publication 800-26 review, agencies can:
1) Continue to use NIST Special Publication 800-26, or,
2) Conduct a self-assessment against the controls found in NIST Special Publication 800-53

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.

2. For each part of this question, identify actual performance in FY 05 by risk impact level and bureau, in the format provided below. From the representative subset of systems evaluated, identify the number of systems which have completed the following: have a current certification and accreditation , a contingency plan tested within the past year, and security controls tested within the past year.

		Question 1						Question 2					
		a. FY 05 Agency Systems		b. FY 05 Contractor Systems		c. FY 05 Total Number of Systems		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and evaluated in the last year		c. Number of systems for which contingency plans have been tested in accordance with policy and guidance	
Bureau Name	FIPS 199 Risk Impact Level	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
ADMN	High	10	0			10	0					0	0.0%
	Moderate	20				20	0					0	0.0%
	Low	7				7	0					0	
	Not Categorized					0	0						
	Sub-total	**37**	**0**	0	0	**37**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
OCIO	High	2	0			2	1					0	0.0%
	Moderate	1		7	0	8	0						
	Low	5				5	0						
	Not Categorized	0				0	0						
	Sub-total	**8**	**0**	7	0	**15**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
CFO	High	8	3			8	3	3	100.0%			1	33.3%
	Moderate	8	1			8	1	1	100.0%			0	0.0%
	Low	2	1			2	1	1	100.0%			1	100.0%
	Not Categorized		0			0	0						
	Sub-total	**18**	**5**	0	0	**18**	**5**	**5**	**100.0%**	**0**	**0.0%**	**2**	**40.0%**
HSG	High	21	2			2	2	2	100.0%			2	
	Moderate	11				11	0					0	
	Low	5				5	0						
	Not Categorized					0	0						
	Sub-total	**37**	**2**	0	0	**37**	**2**	**2**	**100.0%**	**0**	**0.0%**	**2**	**100.0%**
CPD	High	1	1			1	1	1	100.0%			1	100.0%
	Moderate	2				2	0						
	Low	7				7	0						
	Not Categorized	0				0	0						
	Sub-total	**10**	**1**	0	0	**10**	**1**	**1**	**100.0%**	**0**	**0.0%**	**1**	**100.0%**
DEPSEC	High	2	0			2	0					0	0.0%
	Moderate	0				0	0						
	Low	1				1	0						
	Not Categorized	0				0	0						
	Sub-total	**3**	**0**	0	0	**3**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
ENFC	High	1	0			1	0					0	0.0%
	Moderate	0				0	0						
	Low	1				1	0						
	Not Categorized	0				0	0						
	Sub-total	**2**	**0**	0	0	**2**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
FHEO	High	1	1			1	1	1	100.0%			0	0.0%
	Moderate	1				1	0						
	Low	3				3	0						
	Not Categorized	0				0	0						
	Sub-total	**5**	**1**	0	0	**5**	**0**	**1**	**100.0%**	**0**	**0.0%**	**0**	**0.0%**
GNMA	High	0	0	2	0	2	1					0	0.0%
	Moderate	0				0	0						
	Low	0				0	0						
	Not Categorized	0				0	0						
	Sub-total	**0**	**0**	2	0	**2**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
OGC	High	0	0	0	0	0	1					0	0.0%
	Moderate	0				0	0						
	Low	5				5	0						
	Not Categorized	0				0	0						
	Sub-total	**5**	**0**	0	0	**5**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
OIG	High	0	0	2	0	2	0					0	0.0%
	Moderate	0				0	0						
	Low	0				0	0						
	Not Categorized	0				0	0						
	Sub-total	**0**	**0**	2	0	**2**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
PDR	High	0	0	0	0	0	0					0	0.0%
	Moderate	0				0	0						
	Low	0				0	0						
	Not Categorized	0				0	0						
	Sub-total	**0**	**0**	0	0	**0**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
PIH	High	3	1	0	0	3	1	1	100.0%			0	0.0%
	Moderate	0				0	0						
	Low	0				0	0						
	Not Categorized					0	0						
	Sub-total	**3**	**1**	**0**	0	**3**	**1**	**1**	**100.0%**	**0**	**0.0%**	**0**	**0.0%**
REAC	High	4	0	0	0	4	0					0	0.0%
	Moderate	2				2	0						
	Low	4				4	0						
	Not Categorized					0	0						
	Sub-total	**10**	**0**	**0**	0	**10**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
SEC	High	1	0	0	0	1	0					0	0.0%
	Moderate	1				1	0						
	Low	3				3	0						
	Not Categorized					0	0						
	Sub-total	**5**	**0**	**0**	0	**5**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Agency Totals	**High**	**54**	**8**	**4**	**0**	**58**	**8**	**8**	**100.0%**	**0**	**0.0%**	**4**	**50.0%**
	Moderate	**46**	**1**	**7**	**0**	**53**	**1**	**1**	**100.0%**	**0**	**0.0%**	**0**	**0.0%**
	Low	**43**	**1**	**0**	**0**	**43**	**1**	**1**	**100.0%**	**0**	**0.0%**	**1**	**100.0%**
	Not Categorized					**0**		**0**	**0.0%**	**0**	**0.0%**		
	Total	**143**	**10**	**11**	**0**	**154**	**10**	**10**	**100.0%**	**0**	**0.0%**	**5**	**50.0%**

Comments: **1 a) & 2b)** While HUD performed self assessment on two contractor facilities during FY05, none of the 10 systems we reviewed have self assessment completed for FY05. The OCIO has established a September 30, 2005 deadline for the system owners to complete self assessment for their systems. 1b) Since the Department has not identified and included all contractor operated systems on the critical system inventory list, we were not able to include contractor operated systems in our subset system review. 2c) HUD has not developed contingency plans for all systems. HUD has tested contingency plans for 40 out of 154 systems. However, 17 of the 40 systems received tabletop testing only and some of them have high risk impact level. The CISO has indicated that tabletop testing of all mission critical systems will be completed by September 30, 2005. The OCIO will complete tabletop testing for all contingency plans by December 30, 2005.

Question 3

In the format below, evaluate the agency's oversight of contractor systems, and agency system inventory.

3.a.	The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy. Self-reporting of NIST Special Publication 800-26 requirements by a contractor or other organization is not sufficient, however, self-reporting by another Federal agency may be sufficient. Response Categories: - 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	- Mostly, for example, approximately 81-95% of the time
3.b.	The agency has developed an inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency. Response Categories: - Approximately 0-50% complete - Approximately 51-70% complete - Approximately 71-80% complete - Approximately 81-95% complete - Approximately 96-100% complete	- Approximately 81-95% complete
3.c.	The OIG **generally** agrees with the CIO on the number of agency owned systems.	Yes
3.d.	The OIG **generally** agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency.	Yes
3.e.	The agency inventory is maintained and updated at least annually.	Yes
3.f.	The agency has completed system e-authentication risk assessments.	Yes

Comments:**3a** HUD does not maintain a listing of contractor operated information systems. 3b, 3c & 3d) HUD's system inventory does not include all of HUD's applications or the information systems operated for HUD by contractors. (See attached FISMA memo, Section 2 a). 3f) 22 out of 197 HUD systems meet the OMB criteria of "e-government systems" requiring an e-authentication risk assessment and assurance levels. HUD has completed e-authentication risk assessment and assigned an assurance level for all 22 systems. However, HUD did not address the requirements of M-04-04, "E-authentication guidance for Federal Agencies" in the system security plan of systems required E-authentication risk assessment.

Question 4

Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency wide plan of action and milestone (POA&M) process. Evaluate the degree to which the following statements reflect the status in your agency by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the area provided below.

For items 4a.-4.f, the response categories are as follows:

- 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.	- Mostly, for example, approximately 81-95% 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, for example, approximately 81-95% of the time
4.c.	Program officials, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress.	- Mostly, for example, approximately 81-95% of the time
4.d.	CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	- Almost Always, for example, approximately 96-100% of the time
4.e.	OIG findings are incorporated into the POA&M process.	- Almost Always, for example, approximately 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, for example, approximately 96-100% of the time

Comments: HUD has included weaknesses identified during external audits and internal vulnerability assessments in its POA&Ms. However, HUD's system inventory does not include all HUD's applications or some systems operated for HUD by contractors. Therefore, HUD management has neither performed vulnerability assessments nor monitored security weaknesses for these systems. See attached FISMA memo, Section 2a.

Question 5

OIG Assessment of the Certification and Accreditation Process. OMB is requesting IGs to provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. 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 (February, 2004), "Standards for Security Categorization of Federal Information and Information Systems," to determine an impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans .

	Assess the overall quality of the Department's certification and accreditation process. Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	- Satisfactory

Comments: While HUD has determine the risk level for its systems, it has incorrectly categorized a number of its systems. As of 8/30/05, 140 out of 154 HUD systems have been certified and accredited. (See attached FISMA memo, Section 4)

Section B: Inspector General. Question 6, 7, 8, and 9.

Agency Name: U.S. Department of Housing and Urban Development

Question 6

6.a.	Is there an agency wide security configuration policy? Yes or No.	Yes

6.b. Configuration guides are available for the products listed below. Identify which software is addressed in the agency wide security configuration policy. Indicate whether or not any agency systems run the software. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software.

Product	**Addressed in agencywide policy?** **Yes, No, or N/A.**	**Do any agency systems run this software?** **Yes or No.**	**Approximate the extent of implementation of the security configuration policy on the systems running the software.** **Response choices include:** **- Rarely, or, on approximately 0-50% of the systems running this software** **- Sometimes, or on approximately 51-70% of the systems running this software** **- Frequently, or on approximately 71-80% of the systems running this software** **- Mostly, or on approximately 81-95% of the systems running this software** **- Almost Always, or on approximately 96-100% of the systems running this software**
Windows XP Professional	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software
Windows NT	N/A	No	
Windows 2000 Professional	N/A	No	
Windows 2000 Server	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software
Windows 2003 Server	N/A	No	
Solaris	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software
HP-UX	N/A	No	
Linux	N/A	No	
Cisco Router IOS	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software
Oracle	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software
Other. Specify:			

Comments: We performed a review to assess the security of Windows 2000 servers and a review on security configuration of the FHA Unix operating systems during FY05. Also, a HUD contractor performed vulnerability assessments on the General Support Systems that maintain the Unix and Oracle servers during FY05. Configuration weaknesses identified in the reviews and assessments are still open. HUD plans to close most of the Unix and Oracle weaknesses identified in the General Support System assessment by the end of September 2005. There were at least 683 Windows XP Desktops with missing patches. HUD indicated that some of the machines are used for training purposes and the missing patches will be installed upon the next logon to HUD's network. (See FISMA memo, Section 3b).

Question 7

Indicate whether or not the following policies and procedures are in place at your agency. If appropriate or necessary, include comments in the area provided below.

7.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	Yes
7.b.	The agency follows documented policies and procedures for external reporting to law enforcement authorities. Yes or No.	Yes
7.c.	The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov Yes or No.	Yes

Comments: HUD has promulgated policies and procedures for security incidents and violations handling, which address external reporting to law enforcement authorities such as FedCIRC and US-CERT. However, neither HUD's security incident policies and procedures nor its security awareness training provide guidance to HUD users on reporting security incidents to security incident handling team. See attached FISMA memo, Section 3f.		
Question 8		
8	Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? Response Choices include: - Rarely, or, approximately 0-50% of employees have sufficient training - Sometimes, or approximately 51-70% of employees have sufficient training - Frequently, or approximately 71-80% of employees have sufficient training - Mostly, or approximately 81-95% of employees have sufficient training - Almost Always, or approximately 96-100% of employees have sufficient training	- Mostly, or approximately 81-95% of employees have sufficient training
Comments: HUD provided security awareness training to 95% of the total employees and 72% of the total contractors during FY05. However, HUD has not ensured contractors with significant IT security responsibilities received specialized security trainings. See attached FISMA memo, Section 3 c.		
Question 9		
9	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
Comments: HUD forbids the practice of peer-to-peer file sharing. HUD developed policies address the subject and the HUD security awareness training educated its staff on this area.		