U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
Office of Inspector General
451 7th St., S.W.
WASHINGTON, D.C. 20410-4500

MEMORANDUM NO:
2003-DP-0803

September 22, 2003

MEMORANDUM FOR: Vickers B. Meadows, Assistant Secretary for Administration/Chief Information Officer, A

/s/ Hanh Do for
FROM: Curtis Hagan, Director, Information Systems Audit Division

SUBJECT: Annual Evaluation of HUD's Information Security Program

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 HUD's information security program and practices. This memorandum presents the results of our evaluation in accordance with reporting instructions issued by the Office of Management and Budget (OMB).

METHODOLOGY AND SCOPE

Our evaluation is based on our prior audits, audits in progress, network vulnerability testing performed by a HUD subcontractor, and our review of HUD's most recent Plan of Action and Milestones (POA&M). We analyzed HUD's progress in correcting deficiencies reported in the Department's Plan of Action and Milestones and OIG audit reports. We also evaluated HUD's success in accomplishing the goals outlined in the five year IT Security strategic plan for the fiscal years 2002-2006.

BACKGROUND

OMB Memorandum Number M-03-19, dated August 6, 2003, provides reporting instructions for FISMA to federal agencies and Inspectors General. This memorandum requests agency Inspectors General to respond to specific questions in the format provided. Our response is attached.

RESULTS OF REVIEW

We found HUD in general compliance with the requirements of FISMA except for Section 3544(b)(7)(C)(i). This section requires notification of the Office of Inspector General on security incidents. HUD has no procedure for notifying us of security incidents. Furthermore, HUD lacks adequate policies and procedures for documenting incident response activities. In the previous fiscal year (FY 2002), HUD reported 51 Denial of Service Attacks, 24 Probes, and 330 Internet Service Provider Attacks. In FY 2003, only one incident has been reported. Given the number of incidents reported in FY 2002, HUD's network vulnerabilities recently identified by a HUD subcontractor, and the numerous public warnings about worms affecting systems using Microsoft products, there may have been incidents during this fiscal year that have gone unreported.

In our assessment, HUD is not in compliance with OMB Circular A-130, Appendix III, and National Institute of Standards and Technology Special Publication 800-18. Security plans for existing systems have not been updated in a timely manner and security plans for new systems were not developed in a timely manner. There are no current Certifications and Accreditations for the 258 applications listed in HUD's Inventory of Automated Systems.

Based on the testing we performed in our previous audits and audits in progress, improvements are needed in the areas of network security, controls over access to HUD systems, testing of service continuity plans, and overall security program administration.

HUD has taken steps to improve information system security. For example, during this fiscal year HUD implemented a new Microsoft Windows 2000 operating system for its local area network (LAN) servers. HUD is now implementing a new Microsoft Windows XP operating system for employees' desktop personal computers. However, HUD has not taken full advantage of the opportunities presented by these new operating systems to improve security. HUD's password complexity policies do not meet Microsoft recommended settings or NIST guidelines to federal agencies for Windows 2000.

RESPONSES TO OMB QUESTIONS

A.2a. Identify the total number of programs and systems in the agency, the total number of systems and programs reviewed by the program officials and CIOs in FY03, the total number of contractor operations or facilities, and the number of contractor operations or facilities reviewed in FY03. Additionally, IGs shall also identify the total number of programs, systems, and contractor operations or facilities that they evaluated in FY03.						
Bureau Name	**FY03 Programs**		**FY03 Systems**		**FY03 Contractor Operations or Facilities**	
	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed
Office of The Inspector General (OIG)	9	3	258	3	1	1
Office of Chief Information Officer (OCIO)	9	Undetermined	197	Undetermined	1	Undetermined
Agency Total						
b. For operations and assets under their control, have agency program officials and the agency CIO used appropriate methods (e.g., audits or inspections) to ensure that contractor provided services or services provided by another agency for their program and systems are adequately secure and meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy?	Partially (OIG) Yes (OCIO)			Partially (OIG) Yes (OCIO)		
c. If yes, what methods are used? If no, please explain why.	Network Vulnerability Assessment					
d. Did the agency use the NIST self-assessment guide to conduct its reviews?	Partially			Partially		
e. If the agency did not use the NIST self-assessment guide and instead used an agency-developed methodology, please confirm that all elements of the NIST guide were addressed in the agency methodology.	N/A			N/A		

A.2(a) Programs are broken down into the following 9 separate business clusters.

#	Business Cluster	# Of Systems In Cluster
1	Single Family and Multifamily Insurance	20
2	Rental Assistance	10
3	Assessment of HUD Properties	9
4	Provide Grants	11
5	Enforcement FHEO	11
6	Mortgage Backed Securities	4
7	Administrative and Management	153
8	Multiple	33
9	None Indicated	7
	Total Systems	258

Notes:

There was no documentation to support the number of programs, systems or contractor facilities reviewed by the OCIO. We audited application security for two major applications, the Public and Indian Housing Information Center (PIC) and the Tenant Rental Assistance Certification System (TRACS). We also audited LAN network operating system (Windows 2000) security and mainframe computer security. We interviewed HUD officials and reviewed the HUD IT Security Five Year Strategic Plan for the fiscal years 2002 through 2006.

A.2 (b) The NIST Self-Assessment was prepared for all applications and general support systems; therefore, the OIG concluded that HUD has partially incorporated appropriate methodologies to ensure that their programs and systems meet the requirements of FISMA, OMB policy and NIST guidelines. The OMB A-130 review results conducted by a contractor have not been released. The OCIO declined to share a copy of the draft A –130 report with OIG.

A.2 (d) The agency completed only one self-assessment for all applications and general support systems.

A.3. Identify all material weakness in policies, procedures, or practices as identified and required to be reported under existing law in FY03. Identify the number of material weaknesses repeated from FY02, describe each material weakness, and indicate whether POA&Ms have been developed for all of the material weaknesses.

Bureau Name	**FY03 Material Weaknesses**			
	Total Number	Total Number Repeated from FY02	Identify and Describe Each Material Weakness	POA&Ms developed? Y/N
Office of Chief Information Officer (OCIO)	0	0	(1) Security Planning, (2) Certification and Accreditation, (3) Audit Trails	N
Office of the Inspector General (OIG)	3	3	(1) Security Planning, (2) Certification and Accreditation, (3) Audit Trails	N
Agency Total	3	3	(1) Security Planning, (2) Certification and Accreditation, (3) Audit Trails	N

Notes:

A material weakness reported under FISMA does not constitute designation as such for the audit of HUD's financial statements. In addition, these material weaknesses were not designated as such in the latest Federal Managers Financial Integrity Act report.

A.3 (1) Existing system security plans are not updated in a timely manner and security plans for new systems are not developed in a timely manner. Existing security plans for mission critical systems have not been updated every three years as required by OMB Circular A-130, Appendix III and NIST Special Publication 800-18. The OCIO has identified 197 mission critical applications. To date, 17 of the existing security plans have been reviewed with the intent to update the existing plan. Security plans for general support systems have not been updated.

(2) Certifications and Accreditations (C&A) for the 258 applications listed in HUD's Inventory of Automated Systems have expired. HUD plans to request additional financial and human resources to facilitate improvement in the administration of the security program.

(3) Documentation on the use and review of audit trails is poor. Interviews of system owners reveal that the use of audit trails is inconsistent and even when used, the data collected is often not reviewed.

A.4. This question is for IGs only. Please assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestone process that meets the criteria below. Where appropriate, please include additional explanation in the column next to each criteria.	**Yes**	**No**
(1) Agency program officials develop, implement, and manage POA&Ms for every system that they own and operate (systems that support their programs) that has an IT security weakness.	**(Applications)** X	**(General Support Systems)** X
(2) Agency program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress.		X
(3) Agency CIO develops, implements, and manages POA&Ms for every system that they own and operate (systems that support their programs) that has an IT security weakness.	**(Applications)** X	**(General Support Systems)** X
(4) The agency CIO centrally tracks and maintains all POA&M activities on at least a quarterly basis.	X	
(5) The POA&M is the authoritative agency and IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses.		X
(6) System-level POA&Ms are tied directly to the system budget request through the IT business case as required in OMB budget guidance (Circular A-11) to tie the justification for IT security funds to the budget process.	X	
(7) Agency IGs are an integral part of the POA&M process and have access to agency POA&Ms.		X
(8) The agency's POA&M process represents a prioritization of agency IT security weaknesses that ensures that significant IT security weaknesses are addressed in a timely manner and receive, where necessary, appropriate resources.		X

Notes:

A.4 (1). The Inventory of Automated Systems lists applications but not general support systems such as operating systems. The current POA&Ms process does not include development of POA&Ms for the general support systems that are not listed in the inventory.

A.4 (2). The CIO has requested that program officials report quarterly on their progress in correcting weaknesses identified in their respective systems. However, according to the OCIO, the program officials have not been responsive.

A.4 (3). The Inventory of Automated Systems lists applications but not general support systems such as operating systems. The current POA&Ms process does not include development of POA&Ms for the general support systems not listed in the inventory.

A.4 (4). The OCIO has a central listing of POA&Ms and issues a quarterly report.

A.4 (5). In compliance with OMB A-50, we use the Audit Resolution and Corrective Action Tracking System (ARCATS) as a tool for tracking management action on security related weaknesses that we have reported. The CIO uses POA&Ms to identify and manage information and IT Security related weaknesses. However the OCIO does not characterize the system as the authoritative management tool for identifying, and monitoring agency action for the correction of information and IT Security weaknesses. The OCIO also utilizes audits and reviews to identify and monitor information and IT Security related weaknesses.

A.4 (6). System level POA&Ms are used to justify requests for additional resources.

A.4 (7). We (OIG) have access to the POA&Ms, but we have not been an integral part of the POA&M process.

A.4 (8). The POA&M process is not considered a prioritization of agency IT security weaknesses. The POA&M process does not incorporate a priority rating or ranking system.

B.1. Identify and describe any specific steps taken by the agency head to clearly and unambiguously set forth FISMA's responsibilities and authorities for the agency CIO and program officials. Specifically how are such steps implemented and enforced?	The OCIO issued a memorandum on Mar 19, 2003 to Program Officials designating the PMRB members as senior security managers. Secondly the POAM report was issued to Program owners/ IT project leaders for action.
B.2. Can a major operating component of the agency make an IT investment decision without review by and concurrence of the agency CIO?	No
B.3. How does the head of the agency ensure that the agency's information security plan is practiced throughout the life cycle of each agency system?	Capital Planning and Investment Process
B.4. During the reporting period, did the agency head take any specific and direct actions to oversee the performance of 1) agency program officials and 2) the CIO to verify that such officials are ensuring that security plans are up-to-date and practiced throughout the lifecycle of each system?	No
B.5. Has the agency integrated its information and information technology security program with its critical infrastructure protection responsibilities, and other security programs (e.g., continuity of operations, and physical and operational security)?	Yes
B.6. Does the agency have separate staffs devoted to other security programs, are such programs under the authority of different agency officials, if so what specific efforts have been taken by the agency head or other officials to eliminate unnecessary duplication of overhead costs and ensure that policies and procedures are consistent and complimentary across the various programs and disciplines?	No

Notes:

B.1 – The Agency head delegated authority to the CIO to implement and enforce FISMA requirements. The Office of the CIO submitted the POA&M report to system owners and requested corrective action for all of the weaknesses cited for their respective systems. Plans for enforcement are not detailed in the request for corrective action.

B.2 – All IT investments must be approved by the IT investment committee.

B.3 – The CIO is required to integrate system and information security into the Systems Development Methodology to ensure that security is considered throughout the lifetime of the system.

B.4 – There was no documentation available to support any actions taken by the Secretary of HUD.

B.5 – Security is addressed in the critical infrastructure plans and other plans such as the Continuity of Operations Plan (COOP), the Business Resumption Plan (BRP), and OEP.

B.7. Identification of agency's critical operations and assets (both national critical operations and assets and mission critical) and the interdependencies and interrelationships of those operations and assets.				
a. Has the agency fully identified its critical operations and assets, including their interdependencies and interrelationships?	Yes	**X**	No	
b. If yes, describe the steps the agency has taken as a result of the review.	Asked for increased resources			
c. If no, please explain why.	N/A			

Note: B.7 (b). HUD plans to ask for additional human and financial resources to address security program implementation challenges such as complying with OMB A-130, Appendix III on the development and maintenance of system security plans and system certifications and accreditations.

B.8. How does the agency head ensure that the agency, including all components, has documented procedures for reporting security incidents and sharing information regarding common vulnerabilities?				
a. Identify and describe the procedures for external reporting to law enforcement authorities and to the Federal Computer Incident Response Center (FedCIRC).	Undetermined			
b. Total number of agency components or bureaus.	1 (HUD OCIO)			
c. Number of agency components with incident handling and response capability.	1 (HUD OCIO)			
d. Number of agency components that report to FedCIRC.	1 (HUD OCIO)			
e. Does the agency and its major components share incident information with FedCIRC in a timely manner consistent with FedCIRC and OMB guidance?	Undetermined			
f. What is the required average time to report to the agency and FedCIRC following an incident?	Undetermined			
g. How does the agency, including the programs within major components, confirm that patches have been tested and installed in a timely manner?	Regular Penetration Testing and Monitoring Software			
h. Is the agency a member of the Patch Authentication and Distribution Capability operated by FedCIRC?	Yes	X	No	
i. If yes, how many active users does the agency have for this service?	12			
j. Has the agency developed and complied with specific configuration requirements that meet their own needs?	Yes	X	No	
k. Do these configuration requirements address patching of security vulnerabilities?	Yes	X	No	

Notes:

B.8 a – HUD could not produce written policies and procedures that govern incident response to law enforcement, FedCIRC, or the OIG. The OCIO is familiar with the e-mail alerts received from FedCIRC, however, a contractor does all of the reporting to law enforcement and FedCIRC on HUD's behalf. Written policies and procedures for the installation and testing of patches were also not available.

B.8 e - HUD could not produce written policies and procedures that govern incident response to law enforcement, FedCIRC, or the OIG. The OCIO stated that there were no incidents to report in FY 03.

B.8 f - HUD could not produce written policies and procedures that govern incident response to law enforcement or FedCIRC, or the OIG. The OCIO stated that there were no incidents to report in FY 03; therefore, the average time to report to the agency and FedCIRC could not be determined.

B.9. Identify by bureau, the number of incidents (e.g., successful and unsuccessful network penetrations, root or user account compromises, denial of service attacks, website defacing attacks, malicious code and virus, probes and scans, password access) reported and those reported to FedCIRC or law enforcement.		
Bureau Name	Number of incidents reported	Number of incidents reported externally to FedCIRC or law enforcement
OIG	**Undetermined**	**Undetermined**
OCIO	1	1

Note:

B.9 - The Security Awareness Training provided by HUD on September 8th through 10th, 2003 revealed that during FY 02, there were 51 Denial of Service Attacks, 24 Probes, and 330 Internet Service Provider Attacks. Considering this, network vulnerabilities recently identified by a HUD subcontractor, and recent warnings about various worms that attack Microsoft products used by HUD, there may have been incidents during FY 03 that were not reported.

C.1. Have agency program officials and the agency CIO: 1) assessed the risk to operations and assets under their control; 2) determined the level of security appropriate to protect such operations and assets; 3) maintained an up-to-date security plan (that is practiced throughout the life cycle) for each system supporting the operations and assets under their control; and 4) tested and evaluated security controls and techniques? By each major agency component and aggregated into an agency total, identify actual performance in FY03 according to the measures and in the format provided below for the number and percentage of total systems.

Bureau Name	Total Number of Systems	Number of systems assessed for risk and assigned a level or risk		Number of systems that have an up-to-date IT security plan		Number of systems certified and accredited		Number of systems with security control costs integrated into the life cycle of the system		Number of systems for which security controls have been tested and evaluated in the last year		Number of systems with a contingency plan		Number of systems for which contingency plans have been tested	
		No. of Systems	% of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
OCIO	197	17	9	17	9	0	0	197	100	0	0	197	100	0	0
OIG	**258**	**17**	**7**	**0**	**0**	**0**	**0**	**258**	**100**	**0**	**0**	**31**	**12**	**0**	**0**
Agency Total															

Note: C.1 – HUD is in the process of updating 17 security plans for major applications. The plans are in draft form. The Business Resumption Plan specifically states that only the 31 major applications listed in the BRP are covered by the BRP.

C.2. Identify whether the agency CIO has adequately maintained an agency-wide IT security program and ensured the effective implementation of the program and evaluated the performance of major agency components.

Has the agency CIO maintained an agency-wide IT security program? Y/N	Did the CIO evaluate the performance of all agency bureaus/components? Y/N	How does the agency CIO ensure that bureaus comply with the agency-wide IT security program?	Has the agency CIO appointed a senior agency information security officer per the requirements in FISMA?	Do agency POA&Ms account for all known agency security weaknesses including all components?
Yes	NO	**Undetermined**	Yes	NO

Note: We could not determine how the agency ensures that FHA and GNMA comply with HUD's agency wide IT Security program.

C.3. Has the agency CIO ensured security training and awareness of all agency employees, including contractors and those employees with significant IT security responsibilities?							
Total number of agency employees in FY03	Agency employees that received IT security training in FY03		Total number of agency employees with significant IT security responsibilities	Agency employees with significant security responsibilities that received specialized training		Briefly describe training provided	Total costs for providing training in FY03
	Number	Percentage		Number	Percentage		
10,000	10,000	100	200	20	0	Classroom and Intranet	1,000,000

Notes:

C.3 – The 100% figure is a projection based on training in progress.

Agency employees with security responsibilities have access to training programs offered by ESI International, SANS Institute, Global Knowledge, and George Washington University.

C.4. Has the agency CIO fully integrated security into the agency's capital planning and investment control process? Were IT security requirements and costs reported on every FY05 business case (as well as in the exhibit 53) submitted by the agency to OMB?				
Bureau Name	Number of business cases submitted to OMB in FY05	Did the agency program official plan and budget for IT security and integrate security into all of their business cases? Y/N	Did the agency CIO plan and budget for IT security and integrate security into all of their business cases? Y/N	IS IT security costs reported in the agency's exhibit 53 for each IT investment? Y/N
OCIO	35	Yes	Yes	Yes

Distribution Outside HUD

The Honorable Susan M. Collins, Chairman, Committee on Government Affairs,
172 Russell Senate Office Building, Washington, DC 20510
The Honorable Thomas M. Davis, III, Chairman, Committee on Government Reform,
2348 Rayburn Building, House of Representatives, Washington, DC 20515-4611
The Honorable Henry A. Waxman, Ranking Member, Committee on Government Reform,
2204 Rayburn Building, House of Representatives, Washington, DC 20515