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

MEMORANDUM NO.:
2005-DP-0801

October 1, 2004

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

FROM: Curtis Hagan, Director, Information Systems Audit Division, GAA

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 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, 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 (OMB) Memorandum Number M-04-25, dated August 23, 2004, provides reporting instructions for FISMA to Federal agencies and Inspectors General. The memorandum requests agency Inspectors General to respond to specific questions in the format provided. Our responses to OMB questions are within Appendix B, a spreadsheet provided by OMB.

RESULTS OF REVIEW

Our testing found weaknesses in network security that we reported to the Acting Director for IT Operations in a memorandum dated August 6, 2004. Other weaknesses in information system security are reported in our Audit Report titled "Fiscal Year 2004 Review of Information Systems Controls in Support of the Financial Statement Audit." Generally, we reported that improvements are needed in network security, contingency planning for information systems, and the agency-wide information system security program.

In our assessment, HUD has not timely documented and implemented an agency-wide information security program as specified in section 3544(b) of FISMA and has not fully established the minimum set of controls provided in Appendix III to OMB Circular A-130, Security of Federal Automated Information Resources.

However, HUD has taken steps to improve information system security and has made commendable efforts to improve its organization for an effective information system security program.

1. HUD Has Taken Steps To Improve Information System Security.

(a) HUD contracted with the National Institute of Standards and Technology (NIST) in June 2004 to complete a FISMA gap analysis using the Program Review for Information Security Management Assistance (PRISMA) methodology.

(b) HUD has obtained a contractor to provide assistance in developing a strategic computer security plan, reviewing HUD's draft security policies, and the development of a computer security architecture.

(c) HUD initiated new contract actions to update and develop security plans for 170 major business applications.

(d) HUD recently completed a comprehensive review and re-baseline of all HUD applications and systems in the Plan of Action and Milestones. This included reconciliation with information in HUD's Inventory of Automated Systems. In addition, information that was outdated, inconsistent, and duplicative was corrected.

(e) Most HUD employees have completed computer security awareness training.

(f) As of September 27, 2004, HUD had received certification and accreditation packages for 44 out of 187 of its systems from its contractor. The Department expects that all systems will be reviewed by December 31, 2004.

(g) HUD issued a security policy on September 30, 2004 as HUD Handbook 2400.25, *Computer Security Policy Handbook.*

(h) HUD has not had a permanent Senior Security Official to oversee the information system security program. A designated Senior Agency Information Security Officer had been serving in an acting capacity while continuing to perform information technology operations duties. HUD has

not yet created a Senior Agency Information Security Officer position, reporting directly to the Chief Information Officer, tasked with establishing an information security program and empowered with the necessary authority and resources. However, we were informed that on September 30, 2004, HUD detailed an internal consultant with substantial expertise in information systems security to act as a Chief Information Security Officer (CISO) reporting directly to the Chief Information Officer.

2. **HUD Has Not Timely Documented And Implemented An Agency-Wide Information System Security Program As Specified In Section 3544(b) Of FISMA.**

(a) Documentation of the HUD information system security program has not been timely. Documentation of HUD's information security program has been within HUD Handbook Number 2400.24 REV-2. The latest revision is dated November 10, 1999. This date precedes enactment of both FISMA and its predecessor, the Government Information System Security Act (GISRA).

An updated version of the Handbook was drafted in 2003 but not issued. The scope section of Draft HUD Handbook Number 2400.24, REV-3, Security Program Policy, stated:

> This Handbook serves as a supplement to the *HUD Security Program Policy* document. The Handbook contains practical strategic and tactical methodologies, processes, techniques and practices to implement and achieve security objectives defined in the *HUD Security Program Policy* document.

The *HUD Computer Security Policy* document did not exist until drafted in the last week of September 2004. It was issued on September 30, 2004 as HUD Handbook 2400.25, *Computer Security Policy Handbook.*

(b) FISMA requirements for risk assessments have not been met. HUD has not performed adequate risk assessments for all of its networks and systems as required by section 3544(b)(1) of FISMA and by OMB Circular A-130, Appendix III. As discussed in section (e) below, risk assessments for 17 systems have been performed but they did not adequately address the risks, threats, and control environment specific to HUD. Assessments of risk at contractor production and back-up data centers have been performed. HUD has obtained contractor assistance for development of risk assessments for approximately 170 applications in FY 2005.

(c) FISMA requirements for policies and procedures have not been met. HUD policies and procedures (i.e., HUD Handbook) were not based on risk assessments as required by section 3544(b)(2)(A) of FISMA. Periodic risk assessments should provide the Department with opportunities to address security throughout the life cycle of each system as stipulated in section 3544(b)(2)(C) of FISMA. Periodic

risk assessments should also provide the Department with the information necessary to ensure that cost effective procedures are put in place to reduce information security risks to a level acceptable by HUD management as required by section 3544(b)(2)(B) of FISMA.

Requirements within section 3544(b)(2)(D)(ii) of FISMA for compliance with policies and procedures prescribed by OMB and NIST have not been met. For example, applicable NIST guidance had not been incorporated into policies and procedures. While HUD's current, written policy (HUD Handbook Number 2400.24 REV-2) references long-standing OMB policy such as Circular A-130, it did not take into account recent Special Publications (SP) issued by NIST. In fact, HUD Handbook Number 2400.24 REV-2, issued in 1999, did not incorporate NIST guidance issued after the 1995 publication of SP 800-12, *An Introduction to Computer Security*. The HUD Handbook did not incorporate NIST SP 800-18, *Guide for Developing Security Plans for IT Systems,* which was published in 1998. Draft HUD Handbook Number 2400.24, REV-3, which was developed in 2003, did include this NIST publication on a list of references. Neither the draft Handbook nor the current Handbook incorporated more recent NIST guidance such as SP 800-61, *Computer Security Incident Handling Guide*, which was published in January 2004.

The security policy issued on September 30, 2004 as HUD Handbook 2400.25, *Computer Security Policy Handbook*, does incorporate current NIST guidance.

(d) HUD has not documented minimally acceptable system configuration standards as required by FISMA section 3544(b)(2)(D)(iii). The Department contracted with NIST to perform a FISMA gap analysis and make recommendations for security policy and procedures.

(e) FISMA requirements for security plan development have not been met. HUD has not developed security plans for all of its networks and systems as required by section 3544(b)(3) of FISMA. In Audit Report No. 2004-DP-0001, *Fiscal Year 2003 Review of Information Systems Controls in Support of the Financial Statements Audit*, dated December 1, 2003, we reported that "The Department has performed 17 of 258[1] security plan reviews but would not make them available to OIG because they were in draft status." After that audit report was issued, HUD management evaluated the 17 risk assessments upon which the security plans were based and concluded that the risk assessments did not adequately address the risks, threats, and control environment specific to HUD. The 17 risk assessments were eventually provided to us and we also found them to be inadequate. HUD is acting to improve this condition. The Department has awarded a contract for the development of risk assessments in order to facilitate adequate security planning.

[1] The 258 figure was based on the number of systems included in the HUD Inventory of Automated Systems. HUD asserts this figure is misleading in that it includes utilities and minor applications. In FISMA reports for 2003, HUD reported to OMB that it has 197 systems for which security plans should be developed.

(f) Specialized training is needed for key system security personnel. HUD has provided general security awareness training to its employees as required by section 3455(b)(4) of FISMA. However, HUD has not adequately trained all of its security and system administrators in their security responsibilities. For example, in Audit Report No. 2004-DP-0002, *Application Control Review of the Tenant Rental Assistance Certification System*, dated February 25, 2004, we reported that adequate security training had not been provided to key system security personnel.

(g) FISMA requirements for annual testing have not been met. With one exception, HUD does not conduct annual testing and evaluation of the effectiveness of management, operational, and technical controls of information systems within an inventory of systems as required under FISMA section 3544(b)(5). The exception is a contracted-out vulnerability assessment of technical network controls.

(h) FISMA requirements for development and implementation of remedial action have not been met. Although the Department made substantial progress in refining and correcting deficiencies in its Plan of Action and Milestones, it does not have an effective organizational process for remedial action as required by section 3544(b)(6) of FISMA. The Plan of Actions and Milestones has not covered all of the Department's general support systems and the security weaknesses listed on the Plan have not been prioritized for planning corrective action.

(i) FISMA requirements for an incident response program have not been met. The Department has not had written procedures that clearly assign incident response duties and responsibilities and outline the procedures for detecting, responding and reporting on security incidents as required by section 3544(b)(7) of FISMA. The security policy drafted on September 27, 2004 states that HUD shall follow guidelines in NIST 800-61, *Computer Incident Handling Guide*. In our opinion, HUD practices for detecting, reporting, and responding to security incidents have been weak. HUD's intrusion detection tools did not detect an unusually high volume of internal scanning traffic during a recent OIG penetration test.

(j) FISMA requirements for plans and procedures for continuity of systems operations have not been met. Section 3544(b)(8) of FISMA requires that an information security program include plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. In Audit Report No. 2004-DP-0001, *Fiscal Year 2003 Review of Information Systems Controls in Support of the Financial Statements Audit*, dated December 1, 2003, we reported that HUD has a Business Resumption Plan (BRP) equivalent to the Continuity of Support Plan/IT Contingency Plan defined in NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*. However, we also reported:

> While the HUD BRP focuses on IT, the NIST defined BRP is not IT focused and addresses recovering business operations immediately following a disaster. The Department does not

have a Business Continuity Plan (BCP), as defined by NIST, that focuses on sustaining essential business operations while recovering from a significant disruption. The NIST defined BRP and BCP focuses on business processes and addresses IT based only on its support for business processes.

3. Certification and Accreditation Of HUD's Information Systems Are Not Current.

None of HUD's major applications have a current authorization to process transactions as required by OMB Circular A-130, Appendix III, section 3.b(4). HUD does have a certification and accreditation initiative underway for the Department's 197 major applications, system utilities, and general support systems. According to a HUD, the decisions to sign accreditation letters, issue interim authorizations to operate or cease processing are being held in abeyance until each system cluster has been certified within a program office. According to HUD, the reason for withholding these decisions is to ensure consistency of methodology defined by the contractor, who conducted the certification and accreditation, which organized major applications by common platform and program office ownership. According to HUD, while the contractor is generally on schedule, there have been a number of instances where HUD program offices have not or were unable to provide the required security program related documents in order to prepare certification and accreditation packages. As we previously mentioned, HUD has not prepared (1) compliant or current risk assessments and security plans for its major applications, (2) identified all of its general support systems, and (3) prepared or tested a compliant contingency plan. While the Department has recognized the depth and seriousness of the issues facing the IT security program, it has not yet developed or documented policy and procedures to ensure that a regular accreditation and certification process is instituted.

Discussion of Results of Review with HUD

We discussed a draft of this report on September 29, 2004 with representatives from the Office of Administration and the Office of the Chief Information Officer, including the acting Senior Agency Information Security Officer. We made revisions to the report in response to many, but not all, of their verbal comments.

As intended by the guidance in OMB Memorandum Number M-04-25, we have worked closely with HUD officials in developing this report. Due to time constraints, we did not obtain written responses from them for incorporation into this report.

2004 FISMA Report

Agency:	Department of Housing and Urban Development
Date Submitted:	10/1/2004
Submitted By:	OIG

Contact Information:

Name:	Curtis Hagan, Director, ISAD
E-mail:	chagan@hudoig.gov
Phone:	(202) 708-0614 ext. 8149

To enter data in allowed fields, use password: fisma

Section A: System Inventory and IT Security Performance
NOTE: ALL of Section A should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

A.1. By bureau (or major agency operating component), identify the total number of programs and systems in the agency and the total number of contractor operations or facilities. The agency CIOs and IG's shall each identify the total number that they reviewed as part of this evaluation in FY04. NIST 800-26, is to be used as guidance for these reviews.

A.2. For each part of this question, identify actual performance in FY04 for the total number of systems by bureau (or major agency operating component) in the format provided below.

	A.1						A.2									
	A.1.a. FY04 Programs		A.1.b. FY04 Systems		A.1.c. FY04 Contractor Operations or Facilities		A.2.a. Number of systems certified and accredited		A.2.b. Number of systems with security control costs integrated into the life cycle of the system		A.2.c. Number of systems for which security controls have been tested and evaluated in the last year		A.2.d. Number of systems with a contingency plan		A.2.e. Number of systems for which contingency plans have been tested	
Bureau Name	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	Total Number	Percent of Total	Total Number	Percent of Total
Administration	26	14	58	58	2		0						0			
Chief Financial Officer	1	1	20	20			0						0			
Community Planning and Development	1	1	11	11			0						0			
Office of Deputy Secretary	1	1	3	3			0						0			
Enforcement Center	1	1	2	2			0						0			
Fair Housing and Equal Opportunity	1	1	6	6			0						0			
Government National Mortgage Association	1	1	2	2			0						0			
Housing	3	1	42	42			0						0			
General Counsel	1	1	7	7			0						0			
Inspector General	1	1	0	0			0						0			
Policy Development and Research	1	1	1	1			0						0			
Public and Indian Housing	1	1	14	14			0						0			
Real Estate Assessment Center	1	1	12	12			0						0			
Office of Secretary	1	1	9	9			0									
Agency Total	41	27	187	187	0	0	0	0.0%	0	0.0%	0	0.0%	0	0.0%	0	0.0%

Comments	
A.1.a - c	The total number of Bureaus, Systems, and Programs as well as the number reviewed are the figures reported by HUD. We did not attempt to breakdown the number of general support systems we reviewed by bureau or program.
A.2.a	For this information, please see "Results of Review," section 3, of our memorandum.
A.2.b	Security control costs are included in the HUD-prepared A-11 Exhibit 300 Capital Asses Plan and Justification annual budget submitted to OMB.
A.2.c	In FY 2004, the OIG reviewed security controls on HUD's network, mainframes, and followed up on security issues reported from previous reviews of HUD applications.
A.2.d	See "Results of Review" section 2(j) of the accompanying OIG memorandum.
A.2.e	See "Results of Review" section 2(j) of the accompanying OIG memorandum.

A.3. 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 Comment area provided below.	
Statement	**Evaluation**
a. Agency program officials and the agency CIO have used appropriate methods 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.	Rarely, or 0-50% of the time
b. The reviews of programs, systems, and contractor operations or facilities, identified above, were conducted using the NIST self-assessment guide, 800-26.	Almost Always, or 96-100% of the time
c. In instances where the NIST self-assessment guide was not used to conduct reviews, the alternative methodology used addressed all elements of the NIST guide.	Rarely, or 0-50% of the time
d. The agency maintains an inventory of major IT systems and this inventory is updated at least annually.	Almost Always, or 96-100% of the time
e. The OIG was included in the development and verification of the agency's IT system inventory.	Mostly, or 81-95% of the time
f. The OIG and the CIO agree on the total number of programs, systems, and contractor operations or facilities.	Mostly, or 81-95% of the time
g. The agency CIO reviews and concurs with the major IT investment decisions of bureaus (or major operating components) within the agency.	Almost Always, or 96-100% of the time
Statement	**Yes or No**
h. The agency has begun to assess systems for e-authentication risk.	Yes
i. The agency has appointed a senior agency information security officer that reports directly to the CIO.	No

Comments:

A.3.a The HUD CIO has used appropriate methods to ensure that IT policy meet Federal requirements. However, HUD program officials have not used current Federal IT guidance to ensure that they have fulfilled security responsibilities and that their programs and systems are compliant.

A.3.c HUD used NIST SP 800-26 and therefore has no need for alternative methodologies.

A.3.e OIG received regular briefings on HUD's progress in the updating and verification of HUD's IT system inventory. HUD OIG intends to review, monitor, and verify items and actions identified in POA&M starting FY 2005.

A.3.f HUD has not yet finalized the actual number of general support systems and may not have a comprehensive list of systems operated by contractors who are subject to FISMA requirements.

Section B: Identification of Significant Deficiencies
NOTE: ALL of Section B should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

B.1. By bureau, identify all FY 04 significant deficiencies in policies, procedures, or practices required to be reported under existing law. Describe each on a separate row, and identify which are repeated from FY03. In addition, for each significant deficiency, indicate whether a POA&M has been developed. Insert rows as needed.

B.1.				
	FY04 Significant Deficiencies			
Bureau Name	Total Number	Number Repeated from FY03	Identify and Describe Each Significant Deficiency	POA&M developed? Yes or No
Agency Total	0	0		

Comments: See "Results of Review" in the accompanying OIG memorandum.

Section C: OIG Assessment of the POA&M Process
NOTE: Section C should *ONLY* be completed by the OIG. The CIO should leave this section blank.
To enter data in allowed fields, use password: fisma

C.1. 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. This question is for IGs only. 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 Comment area provided below.

C.1	
Statement	**Evaluation**
a. Known IT security weaknesses, from all components, are incorporated into the POA&M.	Almost Always, or 96-100% of the time
b. **Program officials** develop, implement, and manage POA&Ms for systems they own and operate (systems that support their program or programs) that have an IT security weakness.	Rarely, or 0-50% of the time
c. Program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress.	Rarely, or 0-50% of the time
d. **CIO** develops, implements, and manages POA&Ms for every system they own and operate (a system that supports their program or programs) that has an IT security weakness.	Almost Always, or 96-100% of the time
e. CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	Almost Always, or 96-100% of the time
f. The POA&M is the authoritative agency **and** IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses.	Mostly, or 81-95% of the time
g. 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).	Almost Always, or 96-100% of the time
h. OIG has access to POA&Ms as requested.	Almost Always, or 96-100% of the time
i. OIG findings are incorporated into the POA&M process.	Almost Always, or 96-100% of the time
j. POA&M process prioritizes IT security weaknesses to help ensure that significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.	Rarely, or 0-50% of the time

Comments:

C.1.b Program officials do not develop, implement, or manage the POA&M for the systems that they own or operate.

C.1.c Program officials do not report to the CIO on remediation progress.

C.1.f Due to data quality issues, OIG has not used the POA&M as the authoritative tool to track agency actions for correcting information and IT security weaknesses. OIG uses is the Audit Resolution and Corrective Action Tracking System which tracks all findings and recommendations from OIG.

C.1.j The POA&M process does not prioritize IT security weaknesses to ensure they are addressed and receive appropriate resources.

C.1 OIG Assessment of the Certification and Accreditation Process

Section C should only be completed by the OIG. OMB is requesting IGs to assess the agency's certification and accreditation process in order to provide a qualitative assessment of this critical activity. This assessment should consider the quality of the Agency's certification and accreditation process. Any new certification and accreditation work initiated after completion of NIST Special Publication 800-37 should be consistent with NIST Special Publication 800-37. This includes use of the FIPS 199, "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. Earlier NIST guidance is applicable to any certification and accreditation work completed or initiated before finalization of NIST Special Publication 800-37. Agencies were not expected to use NIST Special Publication 800-37 as guidance before it became final.

Statement	Evaluation
Assess the overall quality of the Agency's certification and accreditation process. Comments: See "Results of Review" sections 1(f), 2(b), 2(e), and 3 of the accompanying OIG memorandum.	Poor

Section D
NOTE: ALL of Section D should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

D.1. First, answer D.1. If the answer is yes, then proceed. If no, then skip to Section E. For D.1.a-f, identify whether agencywide security configuration requirements address each listed application or operating system (Yes, No, or Not Applicable), and then evaluate the degree to which these configurations are implemented on applicable systems. **For example:** If your agency has a total of 200 systems, and 100 of those systems are running Windows 2000, the universe for evaluation of degree would be 100 systems. If 61 of those 100 systems follow configuration requirement policies, and the configuration controls are implemented, the answer would reflect "yes" and "51-70%". If appropriate or necessary, include comments in the Comment area provided below.

D.2. Answer Yes or No, and then evaluate the degree to which the configuration requirements address the patching of security vulnerabilities. If appropriate or necessary, include comments in the Comment area provided below.

D.1. & D.2.

	Yes, No, or N/A	Evaluation
D.1. Has the CIO implemented agencywide policies that require detailed specific security configurations and what is the degree by which the configurations are implemented?	No	
a. Windows XP Professional		
b. Windows NT		
c. Windows 2000 Professional		
d. Windows 2000		
e. Windows 2000 Server		
f. Windows 2003 Server		
g. Solaris		
h. HP-UX		
i. Linux		
j. Cisco Router IOS		
k. Oracle		
l. Other. Specify:		
	Yes or No	**Evaluation**
D.2. Do the configuration requirements implemented above in D.1.a-f, address patching of security vulnerabilities?		

Comments:
D.1 See "Results of Review" section 2(a) and 2(d) in the accompanying OIG memorandum.

Section E: Incident Detection and Handling Procedures
NOTE: ALL of Section E should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

E.1. Evaluate the degree to which the following statements reflect the status at your agency. If appropriate or necessary, include comments in the Comment area provided below.

E.1

Statement	Evaluation
a. The agency follows documented policies and procedures for reporting incidents internally.	Rarely, or 0-50% of the time
b. The agency follows documented policies and procedures for external reporting to law enforcement authorities.	Rarely, or 0-50% of the time
c. The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov	Rarely, or 0-50% of the time

E.2.

E.2. Incident Detection Capabilities.

	Number of Systems	Percentage of Total Systems
a. How many systems underwent vulnerability scans and penetration tests in FY04?		

b. Specifically, what tools, techniques, technologies, etc., does the agency use to mitigate IT security risk?

Answer:

Comments:

E.1.a - c See "Results of Review" section 2(i) of the accompanying OIG memorandum. Although there are no documented policies or procedures, HUD does submit weekly incident reports to US-CERT as required.

Section F: Incident Reporting and Analysis
NOTE: ALL of Section F should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

F.1. For each category of incident listed: identify the total number of successful incidents in FY04, the number of incidents reported to US-CERT, and the number reported to law enforcement. If your agency considers another category of incident type to be high priority, include this information in category VII, "Other". If appropriate or necessary, include comments in the Comment area provided below.

F.2. Identify the **number of systems** affected by each category of incident in FY04. If appropriate or necessary, include comments in the Comment area provided below.

F.1., F.2. & F.3.

	F.1. Number of Incidents, by category:			F.2. Number of systems affected, by category, on:		
	F.1.a Reported internally	F.1.b. Reported to US-CERT	F.1.c. Reported to law enforcement	F.2.a. Systems with complete and up to-date C&A	F.2.b. Systems without complete and up to-date C&A	F.2.c. How many successful incidents occurred for known vulnerabilities for which a patch was available?
	Number of Incidents	Number of Incidents	Number of Incidents	Number of Systems Affected	Number of Systems Affected	Number of Systems Affected
I. Root Compromise						
II. User Compromise						
III. Denial of Service Attack						
IV. Website Defacement						
V. Detection of Malicious Logic						
VI. Successful Virus/worm Introduction						
VII. Other						
Totals:	0	0	0	0	0	0

Comments:

F.1.a - c and F2.a - c See "Results of Review" section 2(i) of the accompanying OIG memorandum.

Section G: Training
NOTE: ALL of Section G should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

G.1. Has the agency CIO ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? If appropriate or necessary, include comments in the Comment area provided below.

G.1.

G.1.a. Total number of employees in FY04	G.1.b. Employees that received IT security awareness training in FY04, as described in NIST Special Publication 800-50		G.1.c. Total number of employees with significant IT security responsibilities	G.1.d. Employees with significant security responsibilities that received specialized training, as described in NIST Special Publications 800-50 and 800-16		G.1.e. Briefly describe training provided	G.1.f. Total costs for providing IT security training in FY04 (in $'s)
	Number	Percentage		Number	Percentage		
10,357	9,272	90%			#DIV/0!	Department provided instructor based and web based training to employees and contractors.	$1,006,000

G.2.

	Yes or No
a. Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training?	

Comments:

G.1.c - d HUD OIG believes that the number of employees with significant IT security responsibilities is greater than the number reported by the Department as it may not include program office system administrators and other staff with access to operating systems.