audit report

Issue Date August 22, 2005	
Audit Report Number 2005-DP-0007	

TO: Lisa Schlosser, Chief Information Officer, A

/s/
FROM: Hanh Do, Director, Information System Audit Division, GAA

SUBJECT: Review of HUD's Information Systems Certification and Accreditation Process

HIGHLIGHTS

What We Audited and Why

We audited the quality of the process for certifications and accreditations[1] of the U.S. Department of Housing and Urban Development's (HUD) information systems that were completed through the end of calendar year 2004. We performed this audit as a component of our fiscal year 2005 evaluation of HUD's information security program as specified by the Federal Information Security Management Act.

What We Found

We found that the quality of the process for certification and accreditation of HUD's information systems in calendar year 2004 was poor and that this resulted in presentation of inadequate certification and accreditation packages to the authorizing official. Because the packages were

[1] Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system. Security accreditation is the official management decision to authorize operation of an information system.

incomplete and did not contain the information necessary for the authorizing official to accredit HUD's systems, no accreditations were made in calendar year 2004.

What We Recommend

We recommend that the Chief Information Officer request that the Deputy Secretary appoint senior officials within the program and administrative offices as authorizing officials and direct them to complete certifications and accreditations for their systems in accordance with Office of Management and Budget (OMB) requirements and guidance for Federal agencies published by the National Institute of Standards and Technology (NIST). We also recommend that the Chief Information Officer ensure that policies and procedures for the certification and accreditation process are developed, approved, and implemented and that they address roles and responsibilities assigned during the process.

Auditee's Response

The Chief Information Officer concurs with our finding and all recommendations including recommendations 1A, 1B, and 1C, which were originally addressed to the Deputy Secretary and have since been redirected to the Chief Information Officer. The Deputy Secretary concurs with the three recommendations being redirected to the Chief Information Officer. The complete text of the auditee's comments can be found in appendix A.

TABLE OF CONTENTS

BACKGROUND AND OBJECTIVES

Office of Management and Budget Memorandum Number M-04-25, dated August 23, 2004, on the subject "FY 2004 Reporting Instructions for the Federal Information Security Management Act" requests inspectors generals to assess the agency's certification and accreditation process to provide a qualitative assessment of this critical activity.

Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system. The assessment is made in support of security accreditation and is conducted to determine the extent to which the controls are implemented correctly, operating as intended, and meeting system security requirements.

Accreditation is the official management decision to authorize operation of an information system. By accrediting an information system, an agency official accepts responsibility for the security of the system and is fully accountable for any adverse impacts to the agency if a breach of security occurs. As required by Office of Management and Budget Circular No.A-130, Appendix III, "Security of Federal Automated Information Resources," accreditation provides a form of quality control and challenges managers and technical staffs at all levels to implement the most effective security controls possible in an information system, given mission requirements and technical, operational, cost, and schedule constraints.

The objective of our audit was to assess the quality of the U.S. Department of Housing and Urban Development's (HUD) process for certification and accreditation of its information systems. Our criteria included

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, *Guideline for the Security Certification and Accreditation of Federal Information Systems*.

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems.*

- Office of Management and Budget (OMB) Circular No.A-130, Appendix III, *Security of Federal Automated Information Resources.*

- Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*.

RESULTS OF AUDIT

Finding: The Quality of HUD's Certification and Accreditation Process in 2004 Was Poor, Resulting in Inadequate Certification and Accreditation Packages

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. As a result, no information systems were accredited. For illustration:

- HUD did not appoint senior officials within the program and administrative offices as the authorizing official[2] to formally assume responsibility for operating the various HUD systems. Contrary to OMB Circular A-130 and NIST guidance, the Chief Information Officer (CIO) was designated as the authorizing official for all of HUD's information systems.
- The certifying agent[3] did not conduct detailed security control assessments that extended beyond document reviews.
- System security categorizations were not confirmed with system owners.
- Security certification and accreditation packages did not include completed security assessment reports and final updated security plans.

The quality of HUD's certification and accreditation process suffered from the lack of policies and procedures for performing certifications and accreditations during calendar year 2004. In addition, HUD faced time constraints and pressures that negatively impacted its certification and accreditation process. Facing another failing computer security grade from the House Government Reform Committee due to HUD's lack of certified and accredited information systems, its noncompliance with the Federal Information Security Management Act (FISMA) and noncompliance with OMB Circular A-130, the Department set an aggressive schedule for completion of certifications and accreditations in order to report progress in its annual FISMA report. Despite a clear view of the barriers and time constraints, the Office of the Chief Information Officer proceeded with a process that was unlikely to result in high quality certifications and accreditations but would at least provide a starting point.

As a result, none of HUD's systems were accredited in 2004 and HUD had no assurance that its information security program supports a risk management process.

[2] The authorizing official (or designated approving/accrediting authority as referred to by some agencies) is a senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals.

[3] The certification agent is the individual responsible for conducting the comprehensive evaluation of the management, operational, and technical security controls in the information system.

HUD Did Not Appoint Senior Officials within the Program and Administrative Offices as the Authorizing Officials

HUD has not appointed senior officials within the program and administrative offices as the authorizing officials to formally assume responsibility for operation of HUD systems. The Office of the Chief Information Officer has had to shoulder the responsibility for initiating and executing the certifications and accreditations of HUD's major information systems.

The Acting Chief Information Officer (CIO) drafted an "interim approval to operate" for HUD systems dated December 27, 2004. However, she did not sign the document for any of HUD's systems. The CIO's signature alone on the accreditation document would not have complied with NIST guidelines for accreditation of program office (e.g., Housing, Public and Indian Housing, Chief Financial Officer) information systems. While the guidelines allow the CIO to cosign the accreditation document, a senior official within the program or administrative office must sign the document as the authorizing official. According to NIST Special Publication 800-37, *Guideline for the Security Certification and Accreditation of Federal Information Systems*:

> The authorizing official (or designated approving/ accrediting authority as referred to by some agencies) is a senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals. In some agencies, the senior official and the Chief Information Officer may be co-authorizing officials. In this situation, the senior official approves the operation of the information system prior to the Chief Information Officer. The authorizing official should be someone who has have the authority to oversee the budget and business operations of the information system within the agency and is often called upon to approve system security requirements, system security plans, and memorandums of agreement and/or memorandums of understanding.

Certification and Accreditation Packages Were Incomplete

The certification and accreditation packages that HUD developed did not contain all of the information needed for an accreditation. NIST Special Publication 800-37 indicates that the packages should include (1) an approved system security plan, (2) security assessment report, and (3) plan of action and milestones. HUD's packages did not include final updated security plans or completed security assessment reports, which would have provided a true assessment of the potential risk to the department's operations. The security assessments were inconsistent, fragmented, and limited to document reviews.

The Certification Process Was Deficient

The certification process was deficient in a number of respects:

- Assessments of security controls were based primarily on reviews of out-of-date security plans. There was no indication that procedures such as interviews with system owners, interviews with information technology staff, and observations or testing of controls were performed.

- System security categorizations[4] were not confirmed with system owners even when the categorization designated by the system owners in HUD's inventory of automated systems did not match the categorizations in the system security plans developed by the system owners. The security plans were not current and the inventory of automated systems is not always updated in a timely manner.

- No testing of controls for security was conducted for any information system. General (infrastructure) controls for security were not tested or observed because the certifying agent was denied access to the data center.

[4] The characterization of information or an information system, based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.

- We found that when more than one assessment method was used for certification of an information system, several vulnerabilities were identified. When assessment methods were limited to document reviews, fewer vulnerabilities were identified. A variety of assessment methods, such as interviewing, inspecting, studying, testing, demonstrating, and analyzing, would have resulted in a more thorough review and, in our judgment, would probably have resulted in the identification of additional security vulnerabilities and deficiencies.

- The evaluation of management, operational, and technical controls was inconsistent in that the selection of controls to evaluate varied from one system to another. For example, while an evaluation of operational controls such as "physical and environment protection" and "contingency planning" were evaluated for one system, those same controls were not evaluated for other systems. There were no explanations as to why certain controls were not evaluated.

- The process of assigning scores when evaluating an application system's potential weaknesses was inconsistent, and some high scores (indicating good security) were not warranted.

- Some systems had security plans that were more than three years old and some systems had no security plans. Since security plans were not updated or developed, the packages provided to the authorizing officials did not include final, updated security plans.

- Assessments were based on unapproved criteria (e.g., HUD Handbook No. 2400-24, REV-3). HUD did not have policies and procedures for performing certifications and accreditations during calendar year 2004.

According to NIST Special Publication 800-37, "the system owner should confirm that the security category of the information system has been determined and documented in the system security plan or an equivalent document." As indicated in the publication, the security category of an information system (which should be made in accordance with Federal Information Processing Standards Publication 199[5]) is essential to the certification and accreditation process. It influences the initial selection of security controls from NIST Special Publication 800-53.[6] The level of effort applied to the security certification and accreditation tasks and subtasks should be commensurate with the strength of the security controls

[5] "Standards for Security Categorization of Federal Information and Information Systems," December 2003.

[6] "Recommended Security Controls for Federal Information Systems," January 2005.

selected and the rigor and formality of the assessment methods and procedures selected. As stated in NIST Special Publication 800-37:

> Security certification can include a variety of assessment methods (e.g., interviewing, inspecting, studying, testing, demonstrating, and analyzing) and associated assessment procedures depending on the depth and breadth of assessment required by the agency. . . The identification of vulnerabilities can be accomplished in a variety of ways using questionnaires, on-site interviews, document reviews, and automated scanning tools.

Risks of Not Certifying and Accrediting Information Systems

The certification and accreditation process is a management control for the identification of vulnerabilities that information systems are exposed to. It is also a process for the elimination or mitigation of the vulnerabilities through cost-effective administrative, technical and operational controls. In the absence of this control process, risk is not being managed and it is highly probable that unnecessary risks are being taken.

OMB requires agencies to ensure that security is addressed throughout the budget process. Security must be incorporated into the life-cycle of every information technology investment. To identify the appropriate security controls, agencies must assess the risk to their information and systems. As part of the information technology business case for major systems, agencies report on the risk assessment as well as their compliance with security requirements (e.g., development of security plans and certification and accreditation). Failure to appropriately incorporate security in information technology projects puts funding for the projects at considerable risk.

Operational information technology systems are considered "at-risk" if they are not fully certified and accredited. This can jeopardize HUD's ability to conclude an interagency agreement with other federal or private entities to interface with their information systems. For example, the Department of Health and Human Services required HUD to certify and accredit of one of its systems before it would engage in the computer-matching program that was used to address HUD's material weaknesses in the high-risk rental housing assistance program area.

Conclusion

Having no accreditations, HUD has no assurance that its information security program supports a risk management process, that its information system weaknesses and vulnerabilities have been correctly identified, and that security controls to mitigate those weakness and vulnerabilities have been implemented. Without accreditations, HUD also jeopardizes its ability to conclude interagency agreements on system interfaces as well as receive funding for its information technology projects.

Recommendations

We recommend that the Chief Information Officer:

1A. Request that the Deputy Secretary appoint senior officials within the program and administrative offices to be authorizing officials.

1B. Request that the Deputy Secretary ensure that the authorizing officials complete the certification and accreditation process for their systems.

1C. Request that the Deputy Secretary direct program officials to ensure that the certifications and accreditations are properly conducted in accordance with NIST guidance and that complete and reliable information is provided to the authorizing official to enable him or her to make an informed risk-based decision.

1D. Ensure that policies and procedures for the certification and accreditation process are developed, approved, and implemented and that they address roles and responsibilities assigned during this process.

SCOPE AND METHODOLOGY

We performed the audit

- From February through April 2005,
- In accordance with generally accepted government auditing standards and included tests of internal controls that we considered necessary, and
- At HUD Headquarters, Washington, DC.

Our review focused on certifications and accreditations that were conducted for HUD's application systems in calendar year 2004.

We reviewed applicable guidance and discussed procedures and practices with management and staff personnel with assigned responsibility for certification and accreditation of HUD systems. We reviewed certification and accreditation packages for a sample of five groups of systems from a universe of 58 groups for 176 systems for 17 program offices. The five groups were: (1) Office of Community Planning and Development's Integrated Disbursement and Information System (IDIS), (2) Office of Chief Financial Officer's HUD Central Accounting and Program System (HUDCAPS), (3) Office of Housing's Computerized Homes Underwriting Management System (CHUMS), (4) Office of the Chief Procurement Officer's HUD Procurement System, and (5) Office of Public and Indian Housing's PIH Information Center (PIC). We selected our sample based on (i) importance to HUD's mission and operational responsibilities and (ii) inclusion of systems operated by different offices and on different system platforms.

In our Audit Report No. 2005-DP-0001, "Fiscal Year 2004 Review of Information Systems Controls in Support of the Financial Statements Audit," dated October 19, 2004, we reported that HUD did not meet Office of Management and Budget and Federal Information Security Management Act requirements for periodically assessing risks. At the end of fiscal year 2003, there were no systems with a current (not more than three years old) certification and accreditation. At that time, HUD hired a contractor to assist it in certifying some of its application systems by September 30, 2004. We reported that the agency did not meet the requirements to certify its information systems and that it had not developed standard policies and procedures to support the process. We evaluated previously identified weaknesses as part of this audit and found that many of them still existed.

To complete our objectives, we (1) conducted a compliance review of the HUD certification and accreditation process with National Institute of Standards and Technology federal government recommendations; (2) determined which systems had been certified and accredited; (3) performed a comparison to the National Institute of Standards and Technology to ensure that the certification and accreditation packages included all required documents (i.e., security plans, security assessments, plan of action, and milestones); and (4) assessed the quality and consistency of the certifying agent's evaluation of management, operational, and technical controls.

INTERNAL CONTROLS

Internal control is an integral component of an organization's management that provides reasonable assurance that the following objectives are being achieved:

- Effectiveness and efficiency of operations,
- Reliability of financial reporting, and
- Compliance with applicable laws and regulations.

Internal controls relate to management's plans, methods, and procedures used to meet its mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance.

Relevant Internal Controls

We determined the following internal controls were relevant to our audit objectives:

- Policies, procedures, and control systems used for certifying and accrediting HUD systems.

We assessed the relevant controls identified above.

A significant weakness exists if management controls do not provide reasonable assurance that the process for planning, organizing, directing, and controlling program operations will meet the organization's objectives.

Significant Weaknesses

Based on our review, we believe the following items are significant weaknesses:

HUD did not

- Have written policies and procedures for performing certifications and accreditations during calendar year 2004, which would have provided the program offices and system owners with awareness of their roles, responsibilities, and required level of involvement in the process.

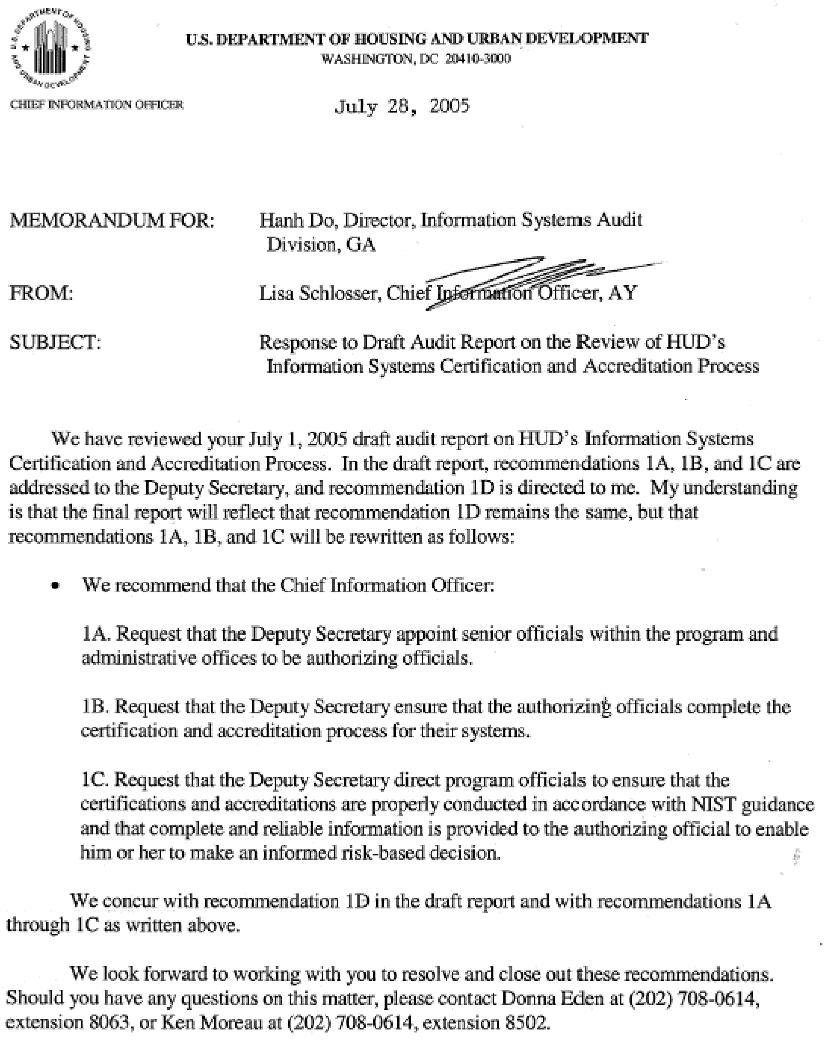
- Provide security certification and accreditation packages to the authorizing official that contained the information necessary for the official to accredit HUD’s application systems. Packages were incomplete due to major time constraints and other limitations.

APPENDIX

Appendix A

AUDITEE COMMENTS AND OIG'S EVALUATION

Refer to OIG Evaluation **Auditee Comments**



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

CHIEF INFORMATION OFFICER

July 28, 2005

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

FROM: Lisa Schlosser, Chief Information Officer, AY

SUBJECT: Response to Draft Audit Report on the Review of HUD's Information Systems Certification and Accreditation Process

Comment 1

We have reviewed your July 1, 2005 draft audit report on HUD's Information Systems Certification and Accreditation Process. In the draft report, recommendations 1A, 1B, and 1C are addressed to the Deputy Secretary, and recommendation 1D is directed to me. My understanding is that the final report will reflect that recommendation 1D remains the same, but that recommendations 1A, 1B, and 1C will be rewritten as follows:

- We recommend that the Chief Information Officer:

  1A. Request that the Deputy Secretary appoint senior officials within the program and administrative offices to be authorizing officials.

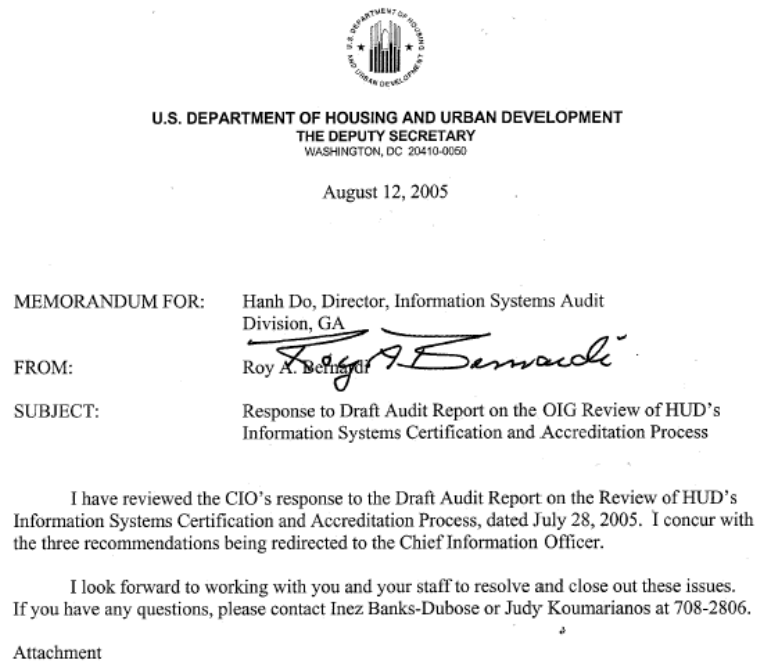
  1B. Request that the Deputy Secretary ensure that the authorizing officials complete the certification and accreditation process for their systems.

  1C. Request that the Deputy Secretary direct program officials to ensure that the certifications and accreditations are properly conducted in accordance with NIST guidance and that complete and reliable information is provided to the authorizing official to enable him or her to make an informed risk-based decision.

We concur with recommendation 1D in the draft report and with recommendations 1A through 1C as written above.

We look forward to working with you to resolve and close out these recommendations. Should you have any questions on this matter, please contact Donna Eden at (202) 708-0614, extension 8063, or Ken Moreau at (202) 708-0614, extension 8502.

Refer to OIG Evaluation **Auditee Comments**



U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
THE DEPUTY SECRETARY
WASHINGTON, DC 20410-0050

August 12, 2005

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

FROM: Roy A. Bernardi

SUBJECT: Response to Draft Audit Report on the OIG Review of HUD's Information Systems Certification and Accreditation Process

Comment 2

I have reviewed the CIO's response to the Draft Audit Report on the Review of HUD's Information Systems Certification and Accreditation Process, dated July 28, 2005. I concur with the three recommendations being redirected to the Chief Information Officer.

I look forward to working with you and your staff to resolve and close out these issues. If you have any questions, please contact Inez Banks-Dubose or Judy Koumarianos at 708-2806.

Attachment

OIG Evaluation of Auditee Comments

Comment 1 The Chief Information Officer concurs with our finding and agrees to implement our recommendations including those recommendations that were originally addressed to the Deputy Secretary and have since been redirected to the Chief Information Officer.

Comment 2 The Deputy Secretary concurs with the three recommendations being redirected to the Chief Information Officer.