



Issue Date
March 24, 2011
Audit Report Number
2011-DP-0006

TO: Douglas A. Criscitello, Chief Financial Officer, F
Mercedes M. Márquez, Assistant Secretary for Community Planning and
Development, D
Jerry E. Williams, Chief Information Officer, Q

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

SUBJECT: HUD's Controls Over Selected Configuration Management Activities Need
Improvement

HIGHLIGHTS

What We Audited and Why

We audited the U.S. Department of Housing and Urban Development's (HUD) controls over selected configuration management (CM) activities. This audit was based on work performed during our fiscal year 2009 and 2010 reviews of information system security controls in support of the annual financial statement audits. During those audits, we identified weaknesses in security controls over selected CM activities.

What We Found

Although HUD had processes and procedures for managing the configurations of systems in HUD's computing environment, those procedures were not always followed. Specifically, (1) CM documentation for the eTravel and Integrated Disbursement and Information System (IDIS) Online systems was outdated, and (2) HUD did not consistently follow its own Configuration Change Management Board (CCMB) review and approval process.

What We Recommend

We recommend that the Office of the Chief Financial Officer update the CM plan for the eTravel system and ensure that contractor support staff reviews application CM documentation at least annually and updates the documentation when changes occur.

We recommend that the Assistant Secretary for Community Planning and Development update the CM plan for IDIS Online and ensure that contractor support staff reviews application CM documentation at least annually and updates the documentation when changes occur.

We recommend that the Office of the Chief Information Officer ensure that all products running on the HUD information technology infrastructure are CCMB approved and that products selected for pilot testing are CCMB approved before conducting the test.

For each recommendation without a management decision, please respond and provide status reports in accordance with HUD Handbook 2000.06, REV-3. Please furnish us copies of any correspondence or directives issued because of the audit.

Auditee's Response

The draft audit report was issued on February 22, 2011, and written comments were requested from each of the report's addressees by March 8, 2011. We received written comments dated March 2, 7 and 14, 2011. The Office of the Chief Financial Officer, Office of Community Planning and Development, and Office of the Chief Information Officer generally agreed with the recommendations in our report.

The complete text of each auditee's response, along with our evaluation of those responses, can be found in appendix A of this report.

TABLE OF CONTENTS

Background and Objectives	4
Results of Audit	
Finding 1: CM Documentation for eTravel and IDIS Online Was Outdated	5
Finding 2: HUD’s CCMB Review and Approval Process Was Not Consistently Followed	9
Scope and Methodology	12
Internal Controls	13
Appendix	
A. Auditee Comments and OIG’s Evaluation	14

BACKGROUND AND OBJECTIVES

The U.S. Department of Housing and Urban Development (HUD) relies extensively on information technology (IT) to carry out its mission and provide services to the American public. Given the prevalence of cyber threats today, HUD must manage its IT assets with due diligence and take the necessary steps to safeguard them while complying with Federal mandates and the dictates of good stewardship.

Within HUD, the Office of the Chief Information Officer (OCIO) is responsible for the security of IT resources. One of the major goals of OCIO is to maintain an enterprise security program that meets all security and privacy-related regulations, statutes, and Federal laws. OCIO coordinates, develops, and implements IT security policy and procedures for HUD.

Configuration management (CM) is one component within the entitywide security program under OCIO's area of responsibility. According to the National Institute of Standards and Technology (NIST), CM provides assurance that the system in operation is the correct version (configuration) of the system and that any changes to be made are reviewed for security implications. CM can be used to help ensure that changes take place in an identifiable and controlled environment and that they do not unintentionally harm any of the system's properties, including its security. To achieve this objective, HUD established the Configuration Change Management Review Board (CCMB) to ensure that all changes made to the HUD IT infrastructure and system development platforms take place through a rational and orderly process.

The Office of the Chief Financial Officer's (OCFO) eTravel system is a critical system that supports HUD's travel needs. eTravel is the Web service interface between the HUD Central Accounting Program System and the FEDTraveler.com system.¹ According to HUD's Inventory of Automated Systems, HUD's Integrated Disbursement and Information System (IDIS) Online is a Web-based grants management system used by the Office of Community Planning and Development (CPD) to automate the administration of grants, including those grants established by the American Recovery and Reinvestment Act of 2009. IDIS Online is used by more than 1,200 HUD grantees, including urban counties and States, to plan activities, draw down program funds, and report on accomplishments. IDIS Online has more than 15,000 individual grantee users as well as several hundred HUD headquarters and field office users.

Our overall objectives were to determine whether (1) CM plans for the selected applications were kept up to date and (2) selected software products followed HUD's CM policies.

¹ FEDTraveler.com is an enterprise solution for Government Travelers.

Finding 1: CM Documentation for eTravel and IDIS Online Was Outdated

CM documentation for eTravel and IDIS Online was not compliant with NIST Special Publication (SP) 800-53² and HUD's own internal policies and procedures. This condition occurred because neither OCFO nor CPD ensured that contractors responsible for maintaining these CM plans kept them up to date in accordance with the most current HUD CM policy, procedures, and template. Because system configuration documentation was not kept up to date, HUD risked providing improper organizational and strategic directions and could not ensure that resource assignments for the implementation would be adequately provided.

CM Documentation Was Outdated

CM documentation for the eTravel and IDIS Online systems was outdated. We reviewed the CM plans for the systems and determined that the plans did not follow CM guidance contained in HUD's Software Configuration Management Policy (Handbook 3252.1) and the HUD software configuration plan template. Plans for both systems lacked information as follows:

- The Roles and Responsibilities section did not include development, test, and production groups that are part of the CM process personnel to ensure proper authorization, testing, approval, and tracking of all configuration changes; and
- The Information section did not include contact information for the supporting groups mentioned above that may be needed for informational and troubleshooting purposes.

In addition, the CM plans for both systems contained outdated information, as outlined in the tables for each system below:

Outdated Information in the eTravel CM Plan	
1	Section 1.3, Project References, contained a reference to the HUD System Development Methodology (SDM), dated August, 2005, although the document had been revised and updated as of January 2009. It also contained a reference to the HUD ADP [automated data processing] Documentation Standards, Handbook 2400.15, which was cancelled in April 2002. However, it did not reference the HUD Software Configuration Management Policy Handbook (3252.1) or the HUD Software Configuration Management Procedures, which are HUD's primary CM documents.

² NIST SP 800-53: Recommended Security Controls for Federal Information Systems and Organization

2	Section 1. 2.1, FedTraveler P221, did not clearly identify the eTravel system environment. It did not identify the vendor for each product used or provide the hardware information for each server or list the operating system. Further, the hardware and software information for the development/test environment should be listed if it is different from the production environment. The CM server information, such as CM tool version and server name, was excluded. In addition, this section and section 2.4, Tools, still listed the old CM tool.
3	Section 1.6, Points of Contact, listed outdated personnel information for the government technical representative. Also, section 1.6.2, Coordination, still listed people who had left HUD. For example, the point of contact for server/operations support had retired, and the point of contact for Office of Information Technology (“OIT-Infrastructure”) had left HUD.
4	The eTravel CM plan did not follow the HUD SDM software configuration plan template. The following sections were missing: Baseline Identification, Measurements, Configuration Status Accounting, Configuration Management Libraries, Release Management, and Configuration Audits. In addition, the plan did not have a System Overview section covering required information such as system environment or special conditions.

Outdated Information in the IDIS Online CM Plan	
1	Section 1.4, Project References, contained references to the HUD Configuration Management Policy, dated February 2001, and the HUD Software Configuration Management Procedures, dated October 2007, although the documents had been revised and updated as of July 2008 and January 2010, respectively. In addition, references to the project management plan, quality assurance plan, and risk assessment plan did not clearly specify whether they referred to IDIS’ plans or other Federal publications. Also, the Integrated Disbursement and Information System Configuration Management Plan, dated January 2006, listed in this section could not be located for verification.
2	Section 1.3, System Overview, did not clearly identify the system environment. It only identified some servers that serve as the hosts for SiteMinder ³ and Lightweight Directory Access Protocol ⁴ as well as the application and database servers. It did not list the servers that host MicroStrategy, which is a business intelligence reporting tool used by IDIS Online, or provide the hardware information for each production server or identify the operating system that the application was running under. Further, the hardware and software information for the development/test environment should be listed since the CM process involves the activities conducted on both development and test servers. The plan also left out its CM server’s information such as CM tool version and server name. In addition, the interface information, such as interface type, data, and frequency of the interfaced applications’ organizations, was not provided.

NIST SP 800-53, section CM-9, Configuration Management Plan, states, “The organization develops, documents, and implements a configuration management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and c.

³ SiteMinder is an authentication and security tool.

⁴ Lightweight Directory Access Protocol is an Internet protocol that e-mail and other programs use to look up information from a server.

Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the items.”

HUD Software Configuration Management Policy Handbook (3252.1), section 3-2, HUD Software Configuration Management Policies, item B, states, “Prepare a SCM⁵ plan for each software project according to the documented procedure for managing the configuration to the software, review it annually, and update it when changes occur. The plan shall comply with HUD SDM Software Configuration Plan template.”

Absent updated documentation, HUD risks that (1) outdated policies and plans may not address current risk and, therefore, be deemed ineffective; (2) programs and program modifications might not be properly authorized, tested, and approved and access to and distribution of programs may not be carefully controlled; and (3) organizational strategic directions and resource assignments for implementation cannot be adequately provided.

Conclusion

CM documentation for eTravel and IDIS Online was not kept up to date. Neither OCFO nor CPD ensured that the contractors responsible for maintaining the eTravel and IDIS Online CM plans kept the information up to date in accordance with the most current HUD CM policy, procedures, and template. If system software CM documentation is not kept up to date, HUD risks providing improper organizational and strategic directions and cannot ensure that resource assignments for implementation will be adequately provided.

Recommendations

We recommend that OCFO

- 1A. Update the CM plan of eTravel to remove references that are obsolete and/or no longer applicable and add all missing information.
- 1B. Ensure that contractor support staff reviews application CM documentation at least annually and update the documentation when changes occur.

⁵ Software Configuration Management

We recommend that the Assistant Secretary for Community Planning and Development

- 1C. Update the CM plan of IDIS Online to remove references that are obsolete and/or no longer applicable and add all missing information.
- 1D. Ensure that contractor support staff reviews application CM documentation at least annually and update the documentation when changes occur.

Finding 2: HUD's CCMB Review and Approval Process Was Not Consistently Followed

HUD did not ensure that its CCMB review and approval process was consistently followed. All software products running in HUD's computing environment had not been CCMB approved, and some products were not CCMB approved before pilot testing. OCIO managers did not believe that software products owned and/or tested by its IT support contractors required CCMB approval. Failure to follow agency policies and procedures for effective agency CM controls increases the risk of potential security impacts due to specific changes to an information system or its surrounding environment.

CCMB Review and Approval Process Was Not Properly Followed

We identified instances within HUD's CM process that demonstrated that HUD did not follow the CCMB review process properly. Specifically,

- Although the majority of software products running in HUD's computing environment went through the formal CCMB process and obtained CCMB approval before their use, the Computer Associates (CA) Unicenter Service Desk (Service Desk),⁶ HUD's help desk application, which has been in use since 2007, was not approved by the CCMB.
- CA Harvest, a software tool for use in the CM of source code and other software development assets, went through multiple pilot tests without prior CCMB approval. Compounding the issue, OCIO's Office of Enterprise Architecture determined in November 2007 that CA Harvest would not meet user needs and moving to CA Harvest would not be cost effective. However, pilot tests were conducted using CA Harvest over a 2-year period, with no request submitted for CCMB review and evaluation of this tool. HUD has demonstrated a history of obtaining CCMB approval for software products before pilot testing, even if the products are ultimately not used.

This condition occurred because the OCIO managers did not believe that software products owned and/or tested by its IT support contractors required CCMB approval.

The HUD Project Leaders Guide to Preparing Submission for the Configuration Change Management Board states that the purpose of a platform configuration change management process is to ensure that all changes made to HUD's IT

⁶ Service Desk is the help desk application used by HUD's IT contractor. The purpose of this application is to provide HUD users with a customer-focused single point of contact for receiving consistent technical support by promptly and efficiently answering calls and providing personal customer assistance. In addition, it automates incident, problem, and change management as well as customer surveys.

infrastructure and system development platforms take place in accordance with a rational and orderly process. It also states that the most critical elements of the CCMB submission are the sections that provide the explanations as to (1) why a change to the IT infrastructure or systems development platform is necessary, (2) how the product or product version proposed to be added to the platform was selected, and (3) what will be involved in implementing the change. It emphasizes that the explanation for the need for change is very important, particularly if there already is a standard established for the general class of products. It states that the submission should address the functionality required that is not provided by the products currently available in the HUD infrastructure, as well as the criteria used to evaluate products, and the results of the evaluation. It strongly recommends that anyone thinking about proposing a new standard come to the CCMB to request concurrence with the idea that a new standard is needed before investing time and effort in researching products and conducting detailed evaluations.

CCMB Classification, approved on May 17, 2006, has defined a pilot lifecycle as “Product/standard to be used in conjunction with technology research efforts only (e.g. testing, pilots).”

The HUD SDM, Version 6.06, Requirements Change, states that requirements changes must be approved by the project CCB (Change Control Board)⁷ before project resources are assigned to implement the change.

NIST SP 800-64, Security Considerations in the System Development Life Cycle, states that an effective agency configuration management and control policy and associated procedures are essential to ensure adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment. Further, it states that configuration management and control procedures are critical to establishing an initial baseline of hardware, software, and firmware components for the information system and subsequently for controlling and maintaining an accurate inventory of any changes to the system. Changes to the hardware, software, or firmware of a system can have a significant security impact. Documenting information system changes and assessing the potential impact on the security of the system on an ongoing basis is an essential aspect of maintaining the security accreditation.

By not consistently following its CCMB approval process and ensuring that all software products are approved for testing and use, HUD increases its risk that products will not meet the needs of its users or the intended purpose of the software and that resources will be unnecessarily expended.

⁷ Change Control Board serves as the decision-making body for each program area project.

Conclusion

OCIO did not ensure that the CCMB review and approval process was consistently followed. OCIO managers did not believe that software products owned and/or tested by its IT support contractors required CCMB approval. Failure to follow the CCMB review process increases HUD's risk that products will not meet the needs of its users or the intended purpose of the software and that resources will be unnecessarily expended.

Recommendations

We recommend that OCIO

- 2A. Ensure that Service Desk is approved by the CCMB.
- 2B. Ensure that all products selected for the pilot test are approved by the CCMB before conducting the test.
- 2C. Ensure that all products running on the HUD IT network infrastructure have obtained CCMB approval.

SCOPE AND METHODOLOGY

The review covered the period October 1, 2008, through September 30, 2010. We performed the audit at HUD headquarters in Washington, DC, from March through November 2010. During our fiscal year 2009 review of information system security controls in support of the annual financial statement audit, we identified inconsistencies and weaknesses in the application of CM policies and procedures at HUD. Consequently, this separate project was initiated to further develop the details of the deficiencies.

Our review was based on guidance from publications by NIST and HUD's own SDM and CM policies and procedures. These publications contain guidance for CM and control. We evaluated controls over the identification and management of security features for hardware, software, and firmware components of an information system

To accomplish our objectives, we reviewed CM policies and procedures and discussed procedures and practices with management and staff personnel responsible for CM.

We conducted the audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

INTERNAL CONTROLS

Internal control is a process adopted by those charged with governance and management, designed to provide reasonable assurance about the achievement of the organization's mission, goals, and objectives with regard to

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

Internal controls comprise the plans, policies, methods, and procedures used to meet the organization's mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations as well as the systems for measuring, reporting, and monitoring program performance.

Relevant Internal Controls

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

- Policies, procedures, control systems, and other management tools used for implementation of security and technical controls for HUD's system security.
- Policies, procedures, controls, and other management tools implemented to detect, prevent, and resolve security incidents.

We assessed the relevant controls identified above.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, the reasonable opportunity to prevent, detect, or correct (1) impairments to effectiveness or efficiency of operations, (2) misstatements in financial or performance information, or (3) violations of laws and regulations on a timely basis.

Significant Deficiency

Based on our review, we believe that the following item is a significant deficiency:


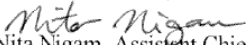
- HUD did not consistently perform CM control activities and monitor implementation of required HUD and NIST policies (findings 1 and 2).

APPENDIX A

OCFO's COMMENTS AND OIG'S EVALUATION

Ref to OIG Evaluation

Auditee Comments

	<p>U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT WASHINGTON, DC 20410-3000</p>
<p>OFFICE OF THE CHIEF FINANCIAL OFFICER ASSISTANT CHIEF FINANCIAL OFFICER FOR ACCOUNTING</p>	<p>MAR 02 2011</p>
<p>MEMORANDUM FOR:</p>	<p>Hanh Do, Director, Information Systems Audit Division, GAA</p>
<p>FROM:</p>	<p> Nita Nigam, Assistant Chief Financial Officer for Accounting, FB</p>
<p>SUBJECT:</p>	<p>Response to the Draft Audit Report Titled, "HUD's Controls Over Selected Configuration Management Activities Need Improvement"</p>
<p>This memorandum is in response to your February 22, 2011 request to the Chief Financial Officer for comments to the Draft Audit Report Titled, "HUD's Controls Over Selected Configuration Management Activities Need Improvement." We have reviewed this report and have provided comments below.</p>	
<p><u>Finding 1: Configuration Management Documentation for eTravel Was Outdated</u> Configuration Management (CM) documentation for eTravel was not compliant with NIST Special Publication (SP) 800-53 and HUD's own internal policies and procedures (Handbook 3252.1). This condition occurred because OCFO did not ensure that contractors responsible for maintaining these CM plans kept them up to date in accordance with the most current HUD CM policy, procedures, and template. Because system configuration documentation was not kept up to date, HUD risked providing improper organizational and strategic directions and could not ensure that resource assignments for the implementation would be adequately provided.</p>	
<p><u>Recommendation 1A:</u> Update the configuration management plan of eTravel to remove references that are obsolete and/or no longer applicable, and add all missing information.</p>	
<p>Comment 1</p>	<p><u>OCFO Response:</u> OCFO agrees to update the configuration management plan of eTravel to remove references that are obsolete and/or no longer applicable, and add all missing information.</p>
<p><u>Recommendation 1B:</u> Ensure that contractor support staff reviews application configuration management documentation at least annually, and update the documentation when changes occur.</p>	
<p>Comment 2</p>	<p><u>OCFO Response:</u> OCFO agrees to ensure that contractor support staff review application configuration management documentation at least annually, and update the documentation when changes occur.</p>
<p>We look forward to working with you and your staff to resolve and close-out the recommendations. If you have any questions or need additional information please contact Nita Nigam at 202-402-6850 or Anna Butler at 202-402-5637.</p>	

OIG Evaluation of OCFO's Comments

Comment 1 OIG agrees with OCFO's comment and planned corrective action.

Comment 2 OIG agrees with OCFO's comment and planned corrective action.

CPD's COMMENTS AND OIG'S EVALUATION

Ref to OIG Evaluation

Auditee Comments

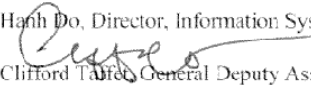


U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
WASHINGTON, DC 20410-7000

OFFICE OF COMMUNITY PLANNING
AND DEVELOPMENT

MAR 14 2011

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

FROM: 
Clifford T. Tate, General Deputy Assistant Secretary for
Community Planning and Development

SUBJECT: CPD Comments on the Draft OIG Audit Report on HUD's
Controls Over Selected Configuration Management
Activities Need Improvement

Community Planning and Development (CPD) appreciates the opportunity to comment on Finding 1: CM Documentation for eTravel and IDIS Online was Outdated. Finding 1 is the only finding that pertains to CPD and its system – Integrated Disbursement and Information System (IDIS) Online.

The report recommends that the Assistant Secretary for CPD update the Configuration Management (CM) plan for the IDIS Online and ensure that contractor support staff review application CM documentation at least annually and updates the documentation when changes occur.

CPD agrees with the Office of Inspector General (OIG) recommendation and met with the IDIS Online contractor, CACI on March 1, 2011 to discuss the updates required for the CM Plan. CPD and CACI agreed that updates for the CM Plan noted by the OIG (Outdated Information in the IDIS Online CM Plan) would be made by June 2011 and subsequently the IDIS Online CM Plan would be updated annually or when system changes require documentation updates. The updates to be made by June 2011 are as follows:

- Section 1.4 Project References will be updated to list the:
 - Latest version of the HUD Configuration Management Policy and the HUD Software Configuration Management Procedures.
 - References to the Project Management Plan, Quality Assurance Plan and Risk Assessment Plan will updated to clearly specify they refer to IDIS Online or other Federal publications.
- Section 1.4 Project References – IDIS Online Configuration Management Plan, dated January 2006 was located and is enclosed.
- Section 1.3 System Overview will be updated to clearly identify the entire system environment including:
 - MicroStrategy servers
 - IDIS Online hardware and operating system for development, test and production servers
 - IDIS Online interface (type, data, and frequency of the interfaced applications' organization) information.

If you have any questions, please contact Valerie D. Coleman at (202) 402-4389.

Comment 1



OIG Evaluation of CPD's Comments

Comment 1 OIG agrees with CPD's comment and planned corrective action.

OCIO's COMMENTS AND OIG'S EVALUATION

Ref to OIG Evaluation

Auditee Comments

	U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT WASHINGTON, DC 20-10-3000
CHIEF INFORMATION OFFICER	MAR 07 2011
MEMORANDUM FOR:	Hanh Do, Director, Information System Audit Division, Office of the Inspector General, GAA
FROM:	Jerry E. Williams, Chief Information Officer, Q 
SUBJECT:	Comments to the Draft Audit Report on HUD's Controls Over Selected Configuration Management Activities Need Improvement
<p>This memorandum is in response to the February 22, 2011, draft audit report entitled, "HUD's Controls Over Selected Configuration Management Activities Need Improvement." My staff and I have reviewed the subject audit report and our comments are provided on the attached.</p> <p>We look forward to working with you and your staff to resolve and close-out the recommendations. Should you have any questions or need additional information, please contact Joyce Little, Director, Office of Investment Strategies Policy and Management at (202) 402-7404.</p> <p>Attachment</p>	

Ref to OIG Evaluation

Auditee Comments

**OCIO Detailed Comments on the Draft Audit Report:
HUD's Controls Over Selected Configuration
Management Activities Need Improvement**

Comment 1

Comment 2

Comment 3

Draft Report Reference	OCIO Management Comments for OIG's Consideration
Page 11, Rec. 2A	<p>Recommendation 2A. Ensure that Service Desk is approved by the CCMB.</p> <p>OCIO concurs with comment:</p> <p>The HITS contract vendor utilizes CA Service Desk Manager to meet their managed services requirements for the HUD National Help Desk that assists and tracks customer service issues. In order to address the reconciliation, OCIO will request that HUD's standard platform information be updated to report CA Service Desk as an approved standard.</p>
Page 11, Rec. 2B	<p>Recommendation 2B. Ensure that all products selected for the pilot test are approved by CCMB before conducting the test.</p> <p>OCIO concurs with recommendation.</p>
Page 11, Rec. 2C	<p>Recommendation 2C. Ensure that all products running on the HUD IT network infrastructure have obtained CCMB approval.</p> <p>OCIO concurs with recommendation.</p>

OIG Evaluation of OCIO's Comments

Comment 1 OIG agrees with OCIO's comments.

Comment 2 OIG agrees with OCIO's comment.

Comment 3 OIG agrees with OCIO's comment.