



| | |
|------------|------------------|
| Issue Date | January 25, 2007 |
|------------|------------------|

| | |
|---------------------|--------------|
| Audit Report Number | 2007-DP-0003 |
|---------------------|--------------|

TO: Joseph Neurauter, Chief Procurement Officer, N

Walter J. Burch for

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

SUBJECT: Review of HUD's Procurement Systems

HIGHLIGHTS

What We Audited and Why

We audited the U.S. Department of Housing and Urban Development (HUD) Procurement System and Small Purchase System to assess their compliance with federal financial management and Federal Information Security Management Act of 2002 (FISMA) requirements. We evaluated the systems and reviewed certain input and processing controls to determine (1) whether the HUD procurement systems comply with the requirements of the Joint Federal Management Improvement Program publication, JFMIP SR-02-02, "Acquisition/Financial Systems Interface Requirements," and (2) the adequacy of the implementation of information security responsibilities and information security categorization. We performed the audit as a component of our fiscal year 2006 consolidated financial statement audit and our annual evaluation of HUD's information security program within the context of FISMA.

What We Found

The HUD Procurement System and Small Purchase System does not adequately support HUD's efforts to manage and monitor procurement transactions. They do not (1) adequately monitor the procurement process, (2) have adequate separation

of duties controls, or (3) contain sufficient financial data to effectively manage and monitor procurement transactions. In addition, HUD's Office of the Chief Procurement Officer did not design or implement information security controls or ensure that its information security responsibilities were fulfilled as required by FISMA and HUD's information technology security policies and procedures.

What We Recommend

We recommend that the Office of the Chief Procurement Officer perform a cost benefit analysis to determine whether it is more advantageous to modify or replace the HUD Procurement System and Small Purchase System to comply with federal requirements. An analysis should be completed to ensure that the resulting systems implement functionality with sufficient financial information to support the primary acquisition functions of fund certification, obligation, deobligation, payment, and closeout. We also recommend that the Office of the Chief Procurement Officer complete, design, and implement the required information security controls.

Auditee's Response

The auditee's response, along with our evaluation of that response, can be found in appendix A of this report. In addition to specific comments related to the audit report, the Office of the Chief Procurement Officer included a remediation plan and detailed transactions which were referenced as "Attachment 1" with their response. The plan and transactions were considered and reviewed but were not included in the report as they pertain to the audit close-out/management decision process.

TABLE OF CONTENTS

| | |
|--|----|
| Background and Objectives | 4 |
| Results of Audit | |
| Finding 1: HUD’s Procurement Systems Do Not Have Adequate Controls for Monitoring the Procurement Process | 5 |
| Finding 2: HUD’s Procurement Systems’ Separation of Duties Controls Were Bypassed | 9 |
| Finding 3: HUD’s Procurement Systems Do Not Contain Sufficient Financial Data to Allow It to Effectively Manage and Monitor Procurement Transactions | 14 |
| Finding 4: The Office of the Chief Procurement Officer Did Not Design or Implement Required Information Security Controls | 18 |
| Scope and Methodology | 26 |
| Internal Controls | 27 |
| Appendixes | |
| A. Auditee Comments and OIG’s Evaluation | 28 |

BACKGROUND AND OBJECTIVES

The U.S. Department of Housing and Urban Development (HUD) Procurement System is an acquisition system that tracks and manages procurement actions through procurement planning, requests for services, solicitation, award, contract administration, and contract closeout for all purchases over \$100,000. HUD's Small Purchase System is used to track purchases of \$100,000 or less. Both systems interface with the HUD's Centralized Accounting and Program System (HUDCAPS) to reserve and obligate funds. HUD uses the systems to (1) monitor workload levels of contracting officers and contract specialists, (2) track events throughout the life of a contract or order (i.e., award, obligation of funds, contract modification, contractor performance, and closeout), (3) identify outstanding procurement requests, and (4) report to the Federal Procurement Data Center to comply with federal requirements so that the Office of Management and Budget and the General Services Administration can manage contracting governmentwide.

The Joint Federal Management Improvement Program publication, JFMIP SR-02-02, "Acquisition/Financial Systems Interface Requirements," addresses the shared information requirements between federal financial and acquisition management systems. It identifies existing governmentwide statutory and regulatory requirements associated with the mutual functional interfaces between finance and acquisition. Appendix A of the guidance includes a complete list of applicable references and authoritative sources. Agencies must use these functional requirements, in addition to agency-unique mission requirements, in planning their financial management and acquisition systems improvement projects. Acquisition/financial management system interface functionality does not necessarily reside in a single software application or functional system. The interface between acquisition and financial management systems information may reside in a number of applications or systems, both automated and manual.

Signed into law in December 2002, the E-Government Act (Public Law 107-347) focuses on the need to address the ever-increasing risk of potential security threats to information and information systems in federal agencies. Title III of the Act, entitled the "Federal Information Security Management Act of 2002" and widely known as FISMA, requires that all federal agencies provide security for the information and information systems that support the operations and assets of the agency, including those managed by other agencies or contractors. FISMA also requires agencies to implement processes to measure information technology security progress and submit quarterly and annual reports to the Office of Management and Budget and Congress, stating progress in areas such as securing information systems and resolving information technology security audit findings.

The objective of this application review of HUD's procurement systems, in addition to the review of certain input and processing controls, was to assess compliance with federal financial management and FISMA requirements. We evaluated (1) whether the HUD procurement systems comply with the requirements of JFMIP SR-02-02 and (2) the adequacy of the implementation of information security responsibilities and information security categorization.

RESULTS OF AUDIT

Finding 1: HUD's Procurement Systems Do Not Have Adequate Controls for Monitoring the Procurement Process

The HUD procurement systems do not have adequate controls to ensure that the data used to monitor the procurement process are accurate. HUD Procurement System and Small Purchase System applications do not have controls to ensure that (1) users do not exceed their procurement authority, (2) only users with procurement authority are authorizing the obligation of funds within the system interface with HUD's Centralized Accounting and Program System (HUDCAPS), and (3) all parties to an acquisition transaction are identified. The conditions exist because the Office of the Chief Procurement Officer did not equate obligating funds in the procurement systems through the HUDCAPS interface with creating a legal obligation for HUD via signing a contract action. Without these controls, HUD management cannot ensure that its procurement systems have complete or accurate information, and monitoring of the procurement process requires a manual review of paper documents, which is inefficient and labor intensive.

There Are No Controls to Prevent Contract Officers from Exceeding Their Procurement Authority

There are no controls within either the HUD Procurement System or Small Purchase System to prevent users with contracting officer authority from exceeding their approved purchase authority. For example, there are no controls within either system that prevent users with up to a \$25,000 procurement authority from entering into the system a transaction for \$1 million. In addition, there is no requirement that contracting officers provide copies of their HUD-issued procurement authority as support for the transactions.

We reviewed all 3,660 funding transactions processed through the HUD Procurement System to the HUDCAPS interface for the period April 1, 2005 through March 31, 2006. We identified four users with procurement authority who processed 24 transactions totaling \$16.1 million in excess of their procurement authority. The HUD Procurement System does not require completion of the contract officer field within the system. In addition, the system does not require that procurement transactions be entered or approved by individuals with the sufficient procurement authority to do so.

| Staff identifier | Number of transactions in which procurement authority was exceeded | Total amount in excess of their procurement authority |
|-------------------------|---|--|
| W ¹ | 4 | \$ 8,503,655 |
| X | 13 | 1,023,603 |
| Y | 2 | 318,088 |
| Z | 3 | 6,231,483 |
| Total | 24 | \$16,139,829 |

The Federal Acquisition Regulation specifies the actions that contracting officers have the authority to perform. Section 1.602-1 states: “(a) Contracting officers have authority to enter into, administer, or terminate contracts and make related determinations and findings. Contracting officers may bind the Government only to the extent of the authority delegated to them. Contracting officers shall receive from the appointing authority in writing the limits of their authority. Information on the limits of the contracting officers’ authority shall be readily available to the public and agency personnel.”

Users Were Granted the Ability to Record Obligations without Contract Officer Review and Approval

Of the 3,660 transactions reviewed, we also identified three users who did not have procurement authority and were granted the ability to enter obligation data into the HUD’s Centralized Accounting and Program System (HUDCAPS) through the HUD Procurement System interface. As stated earlier, there are no requirements that a contracting officer approve or review these transactions within the system. Two of the three users we identified created 149 obligation transactions totaling \$4.8 million, as shown below.

| Staff identifier | Number of transactions processed without procurement authority | Dollars processed |
|-------------------------|---|--------------------------|
| A ² | 7 | \$ 450,207 |
| B | 142 | 4,361,962 |
| Total | 149 | \$4,812,169 |

The Federal Acquisition Regulation, part 1, subpart 1.6, Career Development, Contracting Authority, and Responsibilities, section 1.603-3, Appointment, states: “(a) Contracting officers shall be appointed in writing on an SF [Standard Form] 1402, Certificate of Appointment, which shall state any limitations on the scope of authority to be exercised, other than limitations contained in applicable law or regulation. Appointing officials shall maintain files containing copies of all appointments that have not been terminated.”

¹ Relates to a specific employee and user ID.

² Relates to a specific employee and user ID.

Financial accounting records/entries for procurement transactions should be either created by or with a required system approval of a contract officer. This approval must be made by a contract officer with procurement authority sufficient to approve the transaction and should ensure that the procurement action within the procurement system agrees with the signed contract document.

The Contracting Officer Field Is Not Required

The contracting officer field within the HUD Procurement System is not a required field. The contracting officer is the individual who has the ability to enter into a valid acquisition transaction on behalf of the government. Failure to track this information within the HUD Procurement System application severely limits its usefulness for monitoring the procurement process.

HUD Acquisition Regulation, subpart 2401.6, Career Development, Contracting Authority, and Responsibilities, section 2401.603-3, Appointment, states: “(a) Appointments to an official not expressly delegated procurement authority by a published departmental delegation of authority shall be made in writing by the Head of the Contracting Activity. The Certificate of Appointment (SF 1402) shall constitute the appointing official’s determination that the appointee meets the selection requirements set forth at 2401.603-2.” There are no additional regulations that allow for the further delegation of the procurement responsibilities.

Conclusion

As noted above, current HUD and federal regulations state that the contracting officer is the only individual legally able to obligate the agency. Absent controls to ensure that users cannot exceed their authority and that all parties to the transaction are identified, neither the responsible contracting officer nor HUD management can ensure that its procurement systems have complete or accurate information. Further, without the assurance of complete and accurate information, monitoring of the procurement process requires a manual review of the paper documents, which is inefficient and labor intensive. Without an established and effective internal control program, there cannot be an effective monitoring process. Also, without an effective monitoring capability, HUD cannot provide assurance regarding effective and efficient operations and compliance with applicable laws and regulations.

Recommendations

We recommend that the Office of the Chief Procurement Officer:

- 1A. Review transactions of the four contracting officers who input records in excess of their contract authority and take actions as appropriate.
- 1B. Implement system and procedural controls to ensure that contracting officers are not able to exceed their procurement authority.
- 1C. Implement controls to ensure that contracting officers are required to input, approve, or validate all transactions that record funds through the HUDCAPS interfaces.
- 1D. Modify the systems to make the contracting officer field mandatory.

Finding 2: HUD’s Procurement Systems’ Separation of Duties Controls Were Bypassed

HUD’s procurement systems’ access controls are inadequate. The processing controls allow the Office of the Chief Procurement Officer to bypass certain built-in separation of duties controls within the systems. For example, users were granted multiple user IDs to allow them to process and initiate transactions that were designed to be performed by separate individuals, and user IDs assigned to individuals were not removed from the system when no longer needed due to the creation of group IDs or the inactivation of users’ accounts. These conditions existed because the Office of the Chief Procurement Officer failed to implement an annual review of user access. Absent adequately segregated duties, there is an increased risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, and computer resources damaged or destroyed.

Procurement System Users Were Granted Multiple User IDs to Bypass System Controls

The HUD Procurement System application was designed with built-in segregation of duties controls to prevent a user from having the ability to engage in fraudulent or criminal activity. We identified four users who were granted multiple user ID’s within the system to allow them to bypass the built-in controls. In two of the cases, the user was assigned duties that required the user to act as both the customer and the procurement official for a portion of the transaction. In the other two cases, the users were assigned system administrator access and either procurement official duties or customer duties related to transactions. The following table details the information provided by the Office of the Chief Procurement Officer related to the four users with multiple access to the HUD Procurement System.

| User identifier | Details regarding the user’s access within the HUD Procurement System |
|-----------------|---|
| AA ³ | The user requires a duplicate ID due to having different duties within the system. The user is the government technical representative on the contracts for tax appeals and inspections on multifamily properties in the acquired property disposition inventory and, therefore, needs a customer ID in the system for creating requests for contract services in the system. In order for the user to be able to generate the order numbers in the system, the user has to be in the system as a procurement official. |

³ Relates to a specific employee and user ID.

| User identifier | Details regarding the user's access within the HUD Procurement System |
|-----------------|--|
| BB | The user requires a duplicate ID due to having different duties within the system. The user has a customer ID in the system for creating requests for contract services in the system. The user also holds a contracting officer warrant with responsibilities for executing select contract actions in the system. |
| CC | The user requires a duplicate ID due to having different duties within the system. The user is a system administrator in the system for the appropriate duties for system maintenance and troubleshooting in the field. In addition, the user is a contracting officer with responsibilities for executing contract actions in the system. |
| DD | The user requires a duplicate ID due to having different duties within the system. The user is a system administrator in the system for the appropriate duties for system maintenance and troubleshooting. In addition, the user is the project leader with responsibilities for creating requests for contract services in the system. |

Lack of Routing Functionality within the Small Purchase System Forces Use of Multiple User IDs

We identified 13 users within the HUD Small Purchase System who were assigned multiple user IDs. These IDs were granted because Small Purchase System user IDs are limited in visibility and access is based upon their access level and domain. Records created are usually visible to users with like domains. The Small Purchase System does not contain a routing functionality that allows a user to access the data for more than one domain. Four of the thirteen users have five or more user IDs assigned to them. The issuance of multiple user IDs decreases user productivity, as the user must log out and log in again to access transactions for another location. In addition, it increases the risk that user passwords could be compromised, as users must keep track of multiple login IDs and passwords.

The ability to access transactions for more than one office or region was not an initial requirement of the HUD Small Purchase System. The creation of a domain feature within the system that is similar to the functionality within the HUD Procurement System would require the reprogramming of the underlying search processes programmed within the Small Purchase System to locate data and the modification of the key fields on various tables within the system. The Office of the Chief Procurement Officer did not initiate an enhancement to the system that would create this functionality.

HUD Handbook 2400.25,⁴ section 4.1.3, states: “Program Offices and System Owners shall divide and separate duties and responsibilities of critical IT [information technology] system functions among different individuals to minimize the possibility that any one individual would have the necessary authority or systems access to be able to engage in fraudulent or criminal activity.”

National Institute of Standards and Technology Special Publication 800-14⁵ states: “Early in the process of defining a position, security issues should be identified and addressed to include determining the type of access needed for the position. The two rules that apply for granting access include separation of duties and least privilege. Separation of duties refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process. Least privilege refers to the security objective of granting users only those accesses they need to perform their official duties.”

The Office of the Chief Procurement Officer Did Not Perform Annual User Access Reviews

We identified instances in which users who no longer required it still had access to the HUD Procurement System and Small Purchase System. We identified 11 instances in which HUD Procurement System users were granted two individual user IDs because the user IDs assigned to these individuals were not removed when group user IDs were created to provide the users the access needed. We also identified four HUD Procurement System users with inactive accounts that were not removed. In addition, we identified four users with multiple inactive user accounts for the Small Purchase System application and seven users who were assigned additional user IDs that they did not require.

HUD Handbook 2400.25, REV-1, section 5.1, item (e), Identification and Authentication, requires that user access be reviewed once a year. National Institute of Standards and Technology Special Publication 800-12,⁶ section 10.2.2, states: “While it may initially appear that such reviews should be conducted by systems personnel, they usually are not fully effective. Systems personnel can verify that users only have those accesses that their managers have specified. However, because access requirements may change over time, it is important to involve the application manager, who is often the only individual in a position to know current access requirements.”

⁴ “HUD Information Technology Security Policy.”

⁵ “Generally Accepted Principles and Practices for Securing Information Technology Systems.”

⁶ “An Introduction to Computer Security: The NIST Handbook.”

System and Security Administration Functions Are Not Performed by Separate Individuals

Based upon a review of all users with access to the HUD Procurement System and Small Purchase System applications, we identified three users who have the ability to perform security functions within the two applications. Examples of the actions that these users can perform include adding new users, modifying user access, removing user access, and changing passwords. The same three users are also responsible for troubleshooting issues and performing some maintenance functions within the systems and were granted full access to everything within the system to perform those functions.

Regarding the HUD Procurement System, these users are responsible for teaching new users how the systems work. They assist users in using the interface with HUD's Centralized Accounting and Program System (HUDCAPS) and helping them understand the messages received. They also assist users with the interface to the Federal Procurement Data System-Next Generation⁷ (FPDS-NG). In performance of these functions, these users were granted the ability to modify data within the system.

Regarding the Small Purchase System application, the same three users have the same capabilities. Office of the Chief Procurement Officer staff indicated that with the Small Purchase System, they primarily deal with issues regarding the interface with HUDCAPS. In addition, these three individuals are responsible for entering a date in the system that is provided to them by the Contract Management Review Board.

The system security and administration functions for both systems have been assigned this way since the systems' inception.

The Government Accountability Office's "Federal Information Systems Controls Audit Manual," chapter 3, provides that users should be restricted from performing incompatible functions or functions beyond their responsibility. Management should analyze operations and identify incompatible duties that are then segregated through policies and organizational divisions. The manual also identifies certain functions that are generally performed by different individuals, among which are the data security (security administrator) and data administration (system administrator) functions. The data security function is responsible for

⁷ The Federal Procurement Data Center (FPDC), which is part of the General Services Administration, manages the Federal Procurement Data System – Next Generation (FPDS-NG). FPDS-NG is the central repository of statistical information on federal contracting. FPDC, implemented under Public Law 93-400, provides data for Congress, the Executive branch, the private sector, and the public.

developing security policies, procedures, and guidelines and the adequacy of access controls and service continuity procedures. The data administration function is responsible for planning and administering the data used throughout the entity to include installing, maintaining, and using the entity's databases and database management systems.

Conclusion

Absent adequately segregated duties, there is an increased risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, and computer resources damaged or destroyed. Without an established and effective internal control program, there is no assurance that HUD has an effective monitoring process. HUD does not have the ability to monitor and report control exceptions. Also, without an effective monitoring capability, HUD cannot provide assurance regarding effective and efficient operations and compliance with applicable laws and regulations.

Recommendations

We recommend that the Office of the Chief Procurement Officer:

- 2A. Ensure that system administration and security administration functions are separate.
- 2B. Ensure that staff are not assigned conflicting duties, that separate functions are performed by separate individuals, and that the concept of least privilege is applied.
- 2C. Implement formal policies and procedures to recertify the access granted to users at least annually.
- 2D. Create and implement routing functionality within the Small Purchase System to allow users to be granted access to more than one office or region.

Finding 3: HUD's Procurement Systems Do Not Contain Sufficient Financial Data to Allow It to Effectively Manage and Monitor Procurement Transactions

HUD's use of the HUD Procurement System and Small Purchase System as part of its integrated financial management system does not adequately manage and monitor procurement transactions. There is no payment information within either system or their interfaces with HUD's Centralized Accounting and Program System (HUDCAPS) or an interface with the Program Accounting System (PAS) and Line of Credit Control System (LOCCS) payment system. These conditions occurred because the Office of the Chief Procurement Officer did not envision the HUD Procurement System and Small Purchase System as financial systems. As a result, to complete closeout functions for transactions in both systems, users must manually enter HUDCAPS or LOCCS to obtain the necessary information.

Interfaces with HUDCAPS Do Not Contain Data Elements to Support Payment and Closeout Processes

The Office of the Chief Procurement Officer implemented an automated interface between the HUD Procurement System and HUD's Centralized Accounting and Program System (HUDCAPS) in February 1999. The interface between HUD's Small Purchase System and HUDCAPS was implemented in July 1999. Through these interfaces, users are able to certify fund availability and obligate the funds for transactions within HUDCAPS without having to exit the procurement systems. The data related to the transactions processed in HUDCAPS are then automatically recorded in the procurement systems. However, the related payment functions for procurement transactions are recorded within HUDCAPS only. There are no payment data accessible through the interface between the systems. To obtain payment data related to a transaction recorded in the procurement systems, the user must exit the procurement system and then enter the HUDCAPS system separately. A user responsible for monitoring the transactions processed in this manner is required to have access to each of the systems to manage the status of the procurement action.

HUD Did Not Create Interfaces with PAS and LOCCS

The Office of the Chief Procurement Officer initiated formal plans to build an interface between HUD's procurement systems and the Program Accounting System (PAS) to obtain obligation and commitment data from the Line of Credit Control System (LOCCS) payment system in early fiscal year 2005. The creation of this functionality was delayed because modifications that are needed within LOCCS and PAS to implement the interface have not been completed. PAS provides funding control for most of the HUD grant, loan, and subsidy programs that have funds disbursed through LOCCS. LOCCS interfaces nightly with PAS to detect any new or revised funding data.⁸ The Office of the Chief Financial Officer estimates that the modifications to LOCCS and PAS will be completed sometime in fiscal year 2007. Because there is no automated interface, the processes of fund certification, obligation, deobligation, payment, and closeout of transactions that are paid out of the LOCCS system are all completed separately within either PAS or LOCCS. The information is not maintained in the procurement systems. Processing transactions in this way, HUD risks an increase in errors due to the duplication of data input and monitoring of the procurement process and transactions requiring access to each of these systems.

Federal Regulations Mandate Data Elements That Must Exist in the Acquisition and Financial Systems Interface

The Joint Federal Management Improvement Program publication, JFMIP SR-02-02, "Acquisition/Financial Systems Interface Requirements," specifically lists the data elements that are mandatory and those that provide value-added functionality for each phase of the interface between the acquisition system and the financial system. It separates the elements by the phase of the transactions that occur between the two systems; namely, fund certification, obligation, deobligation, payment, and closeout. We assessed the procurement systems and their interfaces to the financial payment systems at HUD against those data elements that are

⁸ Through the PAS-to-LOCCS interface, LOCCS has the most current funding limits. The PAS interface provides LOCCS with project contract authority as well as access to reservation, obligation, and other accounting information. In turn, LOCCS provides PAS with updates concerning disbursements, receivables, collections, receipts, contract amendments, and U.S. Department of the Treasury schedule confirmation transactions. LOCCS interfaces with the PAS system using a nightly batch process by which LOCCS provides information in PAS transaction format to be processed during the regular PAS overnight process. In turn, LOCCS reads the PAS information and updates the LOCCS database with the changes in authorization that it finds.

mandatory or required for the processes of fund certification, obligation, deobligation, payment, and closeout. According to JFMIP SR-02-02, specific data elements, such as contractor information, payment and invoice information, information regarding the amount of money to be obligated, and the accounts or funds from which they are obligated, should be available within the integrated system to support the management and monitoring of the procurement transaction. Access to receiving reports to show that supplies or services purchased were received and are deemed adequate and that the final invoice was received and paid are examples of the types of data required for the contract closeout function.

HUD's Acquisition and Financial Systems Must Be Linked to Create a Single Integrated Financial Management System

The Federal Financial Management Improvement Act and Office of Management and Budget Circular A-127 specifically provide the vision for a single integrated agencywide financial management system. In support of that vision, the Joint Financial Management Improvement Program publishes requirements documents for financial systems and the financial aspects of mixed systems (such as acquisitions). Agency financial management systems fall into three categories: (1) core financial systems; (2) other financial and mixed systems, including acquisition management systems; and (3) departmental executive information systems (systems that provide management information to all levels of management). These systems must be linked electronically to be effective and efficient. Systems in all three of these categories likely have dependencies upon and some data exchange relation to other information management systems used by the agency, such as project management systems or performance tracking systems.

Financial Data Were Not Incorporated into the Procurement Systems

The Office of the Chief Procurement Officer did not envision the HUD Procurement System or Small Purchase System as financial systems. When the interfaces with the HUD Centralized Accounting and Program System (HUDCAPS) were created, the office determined that there was neither a need nor funds to duplicate the functionality of HUDCAPS within the procurement

systems. The procurement systems were not envisioned to be primary sources of financial management data, and payment data were never part of their design.

Conclusion

The functionality required by the Joint Federal Management Improvement Program does not require the acquisition system to duplicate the functionality within the payment system, only that the acquisition system be able to access the data within the financial system. HUD's failure to include access to the financial information within its interface and to implement an interface with the Program Accounting System (PAS)/Line of Credit Control System (LOCCS) forces the use of a manual paper-based process to (1) initiate the commitment and record the obligation of funds paid out of PAS and LOCCS and (2) review and close out transactions, and staff must obtain financial transaction data from the payment systems separately. As a result, HUD risks that it may not have the necessary information available to make informed decisions about the use of its resources. It also risks an increase in errors due to the duplication of data input.

Recommendations

We recommend that the Office of the Chief Procurement Officer:

- 3A. Perform a cost benefit analysis to determine whether it is more advantageous to modify or replace the procurement systems to ensure compliance with Joint Federal Management Improvement Program requirements.
- 3B. Implement functionality to ensure that there is sufficient information within HUD's procurement systems to support the primary acquisition functions of fund certification, obligation, deobligation, payment, and closeout.

Finding 4: The Office of the Chief Procurement Officer Did Not Design or Implement Required Information Security Controls

HUD's Office of the Chief Procurement Officer did not design or implement information security controls or ensure that its information security responsibilities were implemented as required by the Federal Information Security Management Act (FISMA) and HUD's Information Technology Security Handbook. Specifically, (1) the security classifications for HUD's procurement systems were understated, (2) the HUD Small Purchase System risk assessment was not updated to reflect current conditions, (3) the system security plans for the HUD Procurement System and Small Purchase System were not updated, (4) the contingency plans for the two systems are either outdated or do not contain all the required elements, (5) the Office of the Chief Procurement Officer did not actively participate in the system certification and accreditation process software testing phase completed in fiscal year 2005, (6) there is no target date for completion of the 87 known security vulnerabilities, and (7) the Office of the Chief Procurement Officer did not perform a complete business impact analysis for the HUD Procurement System and Small Purchase System.

These conditions occurred in part because (1) the Office of the Chief Procurement Officer was not aware of its information security duties and responsibilities, (2) security documentation was inadequate, and (3) the Office of the Chief Procurement Officer failed to conduct a complete business impact analysis of the HUD procurement process and the specific roles of the HUD Procurement System and Small Purchase System in that process. These conditions were also impacted by the failure of HUD to complete the implementation of an entitywide risk-based security program. Without the appropriate security controls in place, the Office of the Chief Procurement Officer is not able to fully comply with its FISMA responsibilities.

Procurement Systems Are Not Properly Categorized

HUD's procurement systems' information security category is not consistently categorized on its security documentation, inventory of automated systems, or information security plan of actions and milestones (POA&M). On August 17, 2006, the Office of the Chief Procurement Officer notified the Office of the Inspector General (OIG) that it had recategorized its information systems as "low" impact. However, a previous version of the inventory of automated systems indicated that the procurement systems were categorized as "high" impact for nearly all of fiscal year 2006.

We compared the security categorization in the HUD Procurement System and Small Purchase System security plans, the entries for the HUD inventory of automated systems, and the plan of actions and milestones (POA&M) report for

confidentiality, integrity, and availability. We noted differences as shown below. These categorizations should be identical.

| FIPS 199 | System security plans | System inventory of automated systems | System POA&M (fiscal year 2006, 4th quarter draft) |
|------------------------|------------------------------|--|--|
| Confidentiality | Moderate | Low | Low |
| Integrity | Moderate | Low | Low |
| Availability | Moderate | Low | High |

Federal Information Processing Standards (FIPS) Publication 199⁹ establishes security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Office of Management and Budget Memorandum 06-16, “Protection of Sensitive Agency Data,” emphasizes appropriate categorization and implementation of information security controls in applications with personally identifiable information to ensure appropriate levels of protection. It provides clarifying guidance to agencies on what steps to take to ensure the proper safeguarding of information assets while using information technology.

The Small Purchase System Risk Assessment Was Not Updated

The HUD Small Purchase System risk assessment was not updated to reflect the current conditions that may impact the security of the system. The risk assessment was conducted before the system’s database server was moved from HUD headquarters to the Electronic Data Systems data center in West Virginia.

FIPS Publication 200¹⁰ requires that organizations meet the minimum security requirements in this standard by selecting the appropriate security controls and assurance requirements as described in National Institute of Standards and Technology Special Publication 800-53, “Recommended Security Controls for Federal Information Systems.” The process of selecting the appropriate security controls and assurance requirements for organizational information systems to achieve adequate security is a multifaceted, risk-based activity involving management and operational personnel within the organization. Security categorization of federal information and information systems, as required by FIPS Publication 199, is the first step in the risk management process. After the security categorization process, organizations must select an appropriate set of

⁹ “Standards for Security Categorization of Federal Information and Information Systems.”

¹⁰ “Minimum Security Requirements for Federal Information and Information Systems.”

security controls for their information systems that satisfy the minimum security requirements set forth in FIPS Publication 200.

According to FIPS Publication 200, HUD is required to ensure implementation of the following information systems security controls: access controls; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance of information systems; media protection; physical and environmental planning; personnel security; risk assessment; system and services acquisition; system and communications protection; and system and information integrity.

Security Plans Were Not Updated

The Office of the Chief Procurement Officer did not update or include required information in its application systems security plans. The security plans were not updated after major changes to the applications and their operating environment, a change in the system owner, and a change in system security categorizations. In each of these instances, the Office of the Chief Procurement Officer should have made updates. Also, the system security plans do not identify which security controls have been designated as common security controls and which controls have been designated as system-specific controls.

As noted previously, the HUD Procurement System security plans were not updated to reflect the most recent categorizations. The system has been categorized as “high” impact for system availability according to the most recent system inventory listing provided by the Office of the Chief Information Officer, yet the system security plan still lists the availability of the system as “medium” impact. HUD moved into a new network with its information technology services contractors in January 2005; however, the HUD Procurement System application system’s security plan still uses technical system information and network information under the old HUD Integrated Network (HINET) in the system environment section of the security plan. HUD revised HUD Handbook 2400.25, REV-1, in fiscal year 2005; however, the rules of behaviors still refer to the old version, dated November 10, 1999.

Also, the rules of behaviors are not made available to every user before receiving authorization for access to the systems. The system security plan does not identify which security controls have been designated as common security controls and which controls have been designated as system-specific controls. System owners have been informed that the Office of the Chief Procurement Officer will publish common security controls as part of the information security self-assessment process by the Office of Information Technology. When the

common security controls are identified, system owners will incorporate them into the system security plans. The individual responsible for implementing the common security control is not listed in the system security plan. The risk assessment section was not updated to reflect the risk assessment performed in August 2005.

The HUD Small Purchase System application system's security plan was not updated to reflect the most recent categorization. Also, the security plan was not updated to reflect that the Small Purchase System database server was moved from HUD headquarters to the HUD information technology services data center in fiscal year 2005. The plan still indicates that the server is located at HUD headquarters.

Contingency Plans Were Not Updated

The HUD Procurement System and Small Purchase System application systems' contingency plans are not compliant with federal requirements. They are either outdated or do not include all elements required by Federal Information Processing Standards (FIPS) Publication 200 or National Institute of Science and Technology Special Publication 800-34. The contingency planning process relies upon a manual process in the event of system failure, regardless of the type or length of failure. The contingency plans do not address how offices will communicate, system-generated data will be obtained, or documents will be numbered. The contingency planning supporting documentation does not identify (1) how funding information will be obtained from the HUD Centralized Accounting and Program System (HUDCAPS), Line of Credit Control System (LOCCS), and Program Accounting System (PAS); (2) how that information will be documented for later use; (3) who will perform specific functions and make decisions regarding the processing of information; and (4) how approvals will be obtained.

National Institute of Science and Technology Special Publication 800-34,¹¹ section 3.6, states: "To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. As a general rule, the plan should be reviewed for accuracy and completeness at least annually or whenever significant changes occur to any element of the plan. Certain elements, such as contact lists, will require more frequent reviews."

Although HUD entered into the information technology services contract for supporting its information technology infrastructure services in January 2005, the HUD Procurement System contingency plan had not been updated to reflect the current system environment since October 2003. The system's contingency plan

¹¹ "Contingency Planning Guide for Information Technology Systems."

does not include information regarding the system's interface with the Federal Procurement Data System-Next Generation (FPDS-NG); it only identifies that tabletop testing has been performed, which is not adequate for applications with a "high" impact categorization, and refers to obsolete HUD forms for manual processing. While the HUD Small Purchase System contingency plan was updated in April 2006, the plan does not include a general description of the systems, the alternate facility, and reference to the HUD information technology services data center recovery plan developed by Electronic Data Systems.

According to Office of the Chief Procurement Officer staff, they were waiting on updated training templates from the Office of the Chief Information Officer on what needed to be in a major application's risk assessment and security plan before updating the documents for the HUD Procurement System and Small Purchase System. In addition, staff noted that there was no funding for these activities.

**Participation in the System
Certification and Accreditation
Process Was Inadequate**

The Office of the Chief Procurement Officer did not actively participate in the system certification and accreditation software testing process conducted during fiscal year 2005. In OIG Audit Report No. 2005-DP-0007, "Review of HUD's Information Systems Certification and Accreditation Process," we reported that the quality of the process for certification and accreditation of HUD's information systems was poor. We also reported that HUD's certification and accreditation process had not included adequate testing of information technical controls for its application systems. Despite the absence of this testing, the Office of the Chief Procurement Officer accepted the risk associated with several "high" impact security vulnerabilities related to the list of the mandatory Federal Information Processing Standards (FIPS) Publication 200 information security controls.

No Target Dates Are Scheduled for Correction of POA&M Items, and All Vulnerabilities May Not Be Identified

The Office of the Chief Procurement Officer may not have identified all of its information security vulnerabilities. For example, it did not conduct any tests of the Federal Information Processing Standards (FIPS) Publication 200 technical controls as required by the Federal Information Systems Management Act (FISMA) for application systems categorized as having a “high” or “moderate” impact. These vulnerabilities would not be detected through a document review or self-assessment conducted in accordance with National Institute of Standards and Technology Special Publication 800-26.¹²

There are 87 known information security vulnerabilities contained on the HUD Procurement System and Small Purchase System plans of actions and milestones (POA&M) that remain open. The vulnerabilities relate largely to weaknesses in the security plan, risk assessment, audit trails, system interconnection agreements, and ongoing issues relating to configuration management. In all but four instances, there was no target completion date for addressing the vulnerability; rather, the vulnerabilities were shown in the POA&M as delayed. The security impact levels of the open vulnerabilities are as follows:

- 35 are “high” impact,
- 24 are “moderate” impact, and
- 28 are “low” impact.

Additionally, the Office of the Chief Procurement Officer did not test the required controls from the FIPS Publication 200 technical information security control family. This testing is required for all applications that have a “high” security impact categorization, which the HUD Procurement System and Small Purchase System had at certain times during the review period.

The Office of the Chief Procurement Officer Did Not Conduct a Complete Business Impact Analysis

The Office of the Chief Procurement Officer did not perform a complete business impact analysis for the HUD Procurement System and Small Purchase System. The performance of a business impact analysis serves to correlate specific application components with the critical services that they provide and, based on

¹² “Security Self-Assessment Guide for Information Technology Systems.”

that information, to characterize the consequences of a disruption to the application components. It is used to establish HUD's actions in the event that the contingency plan is activated. National Institute of Standards and Technology Special Publication 800-34 requires that a business impact analysis be completed and that the results be incorporated into the strategy development efforts for the organization's continuity of operation plan, business continuity plan, and business resumption plan. Key personnel within the Systems Division of the Assistant Chief Procurement Officer for Policy and Systems stated that although they initiated the process of conducting the business impact analyses, they did not complete the analyses because they were unsure of how to complete them. Despite this uncertainty, they did not contact Office of the Chief Information Officer staff for guidance or assistance.

National Institute of Standards and Technology Special Publication 800-34, section 3.2, Conduct the Business Impact Analysis (BIA), states: "The BIA is a key step in the contingency planning process. The BIA enables the Contingency Planning Coordinator to fully characterize the system requirements, processes, and interdependencies and use this information to determine contingency requirements and priorities. The BIA purpose is to correlate specific system components with the critical services that they provide, and based on that information, to characterize the consequences of a disruption to the system components. Results from the BIA should be appropriately incorporated into the analysis and strategy development efforts for the organization's COOP [continuity of operation plan], business continuity plan, and business resumption plan."

Conclusion

Without the appropriate training, experience, and resources, the Office of the Chief Information Officer is not able to ensure that its systems comply with HUD's information security policies and other federal requirements. Also, the office is not able to comply with the Federal Information Security Management Act (FISMA) responsibilities related to information security, which HUD has delegated to the system owner. For example, by not completing the design or implementation of required information security controls over its procurement application systems, it has not provided adequate information security protections over its data and information system. Failure to perform a complete business impact analysis leaves HUD unable to reliably estimate the impact of a system failure or the amount of time needed to recover from a contingency. Without a business impact analysis, the Office of the Chief Procurement Officer will not have identified the critical resources needed to respond, the potential outage impact, and allowable outage times or develop the recovery priorities needed to develop a compliant contingency plan.

Recommendations

We recommend that the Office of the Chief Procurement Officer:

- 4A. Obtain the training and or resources necessary to develop or perform compliant (1) information system categorization analyses; (2) risk assessments; (3) security plans; (4) contingency plans and tests; (5) monitoring processes, which include applicable Federal Information Processing Standards (FIPS) Publication 200 managerial, operational, and technical information security controls; and (6) evaluations of the managerial, operational, and technical security controls.
- 4B. Complete the corrective actions for the known open information security vulnerabilities or develop mitigation strategies if new system development is underway.
- 4C. Designate a manager to assume responsibility for ensuring the Office of the Chief Procurement Officer's compliance with federal certification and accreditation process requirements and to provide "continuous monitoring" of the office's information systems security.
- 4D. Reevaluate the HUD Procurement System and Small Purchase System application systems' security categorization in light of Office of Management and Budget guidance on personally identifiable information.
- 4E. Perform a business impact analysis for the procurement systems. Based on the results of the impact analysis, determine what actions HUD can take to limit the amount of time needed to recover from the various levels of contingencies that can occur and include the determined actions in the contingency plans for the systems.

SCOPE AND METHODOLOGY

We performed the audit

- From January through September 2006.
- At HUD headquarters, Washington, DC, and the Michigan state office.
- In accordance with generally accepted government auditing standards.

Our assessment focused on the interface requirements between acquisition and financial systems detailed in the Joint Federal Management Improvement Program publication, JFMIP SR-02-02, “Acquisition/Financial Systems Interface Requirements,” and the Federal Information Security Management Act (FISMA) requirements of Title III of the E-Government Act (Public Law 107-347). We reviewed the information security controls and compliance with federal financial management interface requirements of HUD’s procurement systems. We examined system data from the HUD Procurement System and Small Purchase System for the period April 1, 2005, through March 31, 2006.

To accomplish our objectives, we reviewed policies and procedures, interviewed HUD employees from the Office of the Chief Procurement Officer and the Office of the Chief Financial Officer, interviewed Electronic Data Systems’ contract staff, and obtained and analyzed supporting documentation.

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:

- Compliance with federal financial management interface requirements related to payment.
- Design and implementation of information security controls.

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:


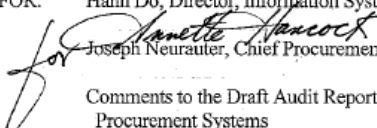
- HUD's procurement systems are inadequate for monitoring the procurement process (finding 1).
- HUD's procurement systems' access controls are inadequate (finding 2).
- HUD's procurement systems do not contain sufficient financial data to allow it to effectively manage and monitor procurement transactions (finding 3).
- The Office of the Chief Procurement Officer has not designed or implemented required information security controls (finding 4).

Appendix A

AUDITEE COMMENTS AND OIG'S EVALUATION

Ref to OIG Evaluation

Auditee Comments

| | |
|---|--|
|  | U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT WASHINGTON, D.C. 20410-3000 |
| OFFICE OF THE CHIEF PROCUREMENT OFFICER | DEC 22 2006 |
| MEMORANDUM FOR: | Hanh Do, Director, Information Systems Audit Division, GAA |
| FROM: |  Joseph Neurauter, Chief Procurement Officer, N |
| SUBJECT: | Comments to the Draft Audit Report – Review of HUD's Procurement Systems |
| <p>This memorandum is in response to your November 16, 2006 draft audit report entitled, "Review of HUD's Procurement Systems." As you are aware, the Office of the Chief Procurement Officer (OCPO) staff met with your staff, either in person or via teleconference, on several occasions to discuss the contents of the draft report. In general, the OCPO agrees with the Office of the Inspector General's findings except as noted in the attached comments. Also, included as an attachment is the OCPO plan to remediate the deficiencies noted in the draft report.</p> <p>We thank you for the opportunity to review the draft report and provide clarification where it is needed. We are looking forward to seeing our comments included in the final report and working with you and your staff to resolve and close out the recommendations. Should you have any questions or need additional information, please do not hesitate to contact Ms. Linda Hooks, OCPO Audit Liaison Officer, at extension 5474.</p> | |
| Attachment (s) | |

Ref to OIG Evaluation

Auditee Comments

Comments on OIG’s Review of HUD’s Procurement Systems

Comment 1

| Report Page Reference | OCPO Comments to OIG’s Report |
|-----------------------|---|
| Page 5 | <p><u>Audit Finding 1:</u> HUD Procurement System and Small Purchase System applications do not have controls to ensure that: (1) users do not exceed their procurement authority</p> <p><u>OCPO Comment:</u> Legal obligation of funds occurs when the contracting officer executes a contract action. HPS is a management system that tracks the processing of procurement actions. Obligations are recorded, not legally created, in the system. A user other than the contracting officer may enter data on a transaction, for example, a procurement technician or contract specialist. As a result, it is not appropriate for HPS to control for the user’s procurement authority. However, we recognize the OIG’s concern that OCPO needs procedures to assure that HUD contracting officers do not exceed their procurement authority or enter into other inappropriate actions (e.g. anti-deficiency). Some controls do exist, particularly that supervisors are cognizant of limits on a staff member’s authority when assigning work and monthly reports to managers that summarize actions completed (which would let a manager identify any anomalous action). We will document existing procedural controls, strengthen them where necessary, and initiate Procurement Management Reviews that will address this concern. With the replacement system, we anticipate improved automated controls.</p> |
| Page 5 | <p><u>Audit Finding 1:</u> HUD Procurement System and Small Purchase System applications do not have controls to ensure that: . . . (2) only users with procurement authority are authorizing the obligation funds within the system interface with HUD’s Central Accounting and Program System (HUDCAPS).</p> <p><u>OCPO Comment:</u> Legal obligation of funds occurs when the contracting officer executes a contract action. HPS is a management system that tracks the processing of procurement actions. Obligations are recorded, not legally created, in the system. A user other than the contracting officer may enter data on a transaction, for example, a procurement technician or contract specialist.</p> |
| Page 5 and 6 | <p><u>Audit Finding 1:</u> There Are No Controls to Prevent Contract Officers from Exceeding Their Procurement Authority</p> <p><u>OCPO Comment:</u> OCPO conducted a review of the specific transactions identified by the IG regarding users exceeding their procurement authority. In light of when the obligation occurs, at contract execution, the OCPO has concluded that all actions were properly executed by contracting officers acting with their authority. Please see Attachment 1, which identifies those transactions reviewed by the OCPO to determine if procurement authority was exceeded.</p> |

Comment 2

Comment 3

Ref to OIG Evaluation

Auditee Comments

| Comments on OIG's Review of HUD's Procurement Systems | |
|---|---|
| Report Page Reference | OCPO Comments to OIG's Report |
| Comment 4 | <p>Page 6</p> <p><u>Audit Finding 1:</u> Users Were Granted the Ability to Record Obligations without Contract Officer Review and Approval.</p> <p><u>OCPO Comment:</u> OCPO conducted a review of the specific transactions identified by the IG regarding users ability to record obligations without contract officer review and approval. In light of when the obligation occurs, at contract execution, the OCPO has concluded that all actions were appropriately performed. Please see Attachment 1, which identifies those transactions reviewed by the OCPO to determine if obligations were recorded without contracting officer validation.</p> |
| Comment 5 | <p>Page 8</p> <p><u>Audit Recommendation 1A:</u> Review transactions of the four contracting officers who input records in excess of their contract authority and take actions as appropriate.</p> <p><u>OCPO Comment:</u> OCPO conducted a review of the specific transactions identified by the IG regarding contracting officers who input records in excess of their contract authority. In light of when the obligation occurs, at contract execution, the OCPO has concluded that all actions were properly executed by contracting officers acting with their authority. Please see Attachment 1, which identifies those transactions reviewed by the OCPO to determine if contracting officer exceeded their contractual authority.</p> |
| Comment 6 | <p>Page 8</p> <p><u>Audit Recommendation 1B:</u> Implement system controls to ensure that contracting officer are not able to exceed their procurement authority.</p> <p><u>OCPO Comment:</u> OCPO recommends inserting "and procedural" following "system." We are not sure an automated system can effectively control the variety of limitations that may exist among contracting officer warrants. However, we will consider this capability in acquiring a replacement system for HPS/SPS. We believe procedural controls are also a necessary element. As stated earlier, we will document existing procedural controls, strengthen them where necessary, and initiate Procurement Management Reviews that will address this concern.</p> |
| Comment 7 | <p>Page 8</p> <p><u>Audit Recommendation 1C:</u> Implement controls to ensure that contracting officers are required to either input or approve all transactions that record funds through the HUDCAPS interfaces.</p> <p><u>OCPO Comment:</u> OCPO recommends changing "either input or approve" to "validate." As part of the procedural controls established in response to 1B, we will have contracting officers validate transactions entered into HPS.</p> |

Ref to OIG Evaluation

Auditee Comments

Comment 8

Comment 9

Comment 10

Comment 11

| Comments on OIG's Review of HUD's Procurement Systems | |
|---|--|
| Report Page Reference | OCPO Comments to OIG's Report |
| Page 8 | <p><u>Audit Recommendation 1D</u>: Modify the systems to make the contracting officer field mandatory.</p> <p><u>OCPO Comment</u>: OCPO will implement procedures to require that contracting personnel complete the contracting officer field and provide reports to identify records where this field is not complete. However, as OCPO anticipates acquiring a replacement system, we will not reprogram the existing HPS but will consider this as a requirement for the replacement system.</p> |
| Page 13 | <p><u>Recommendation 2A</u>: Ensure that system administration and security administration functions are separate</p> <p><u>OCPO Comment</u>: The OCPO will formally appoint separate individuals to act as security administrator and system administrator for each OCPO system and establish procedures to ensure that the individuals will not perform conflicting duties. However, these actions will be manual for the current HPS and SPS (see comment on Recommendation 2B). As OCPO anticipates acquiring a replacement system, we will include this capability in the requirements for the replacement system.</p> |
| Page 13 | <p><u>Recommendation 2B</u>: Ensure that staff are not assigned conflicting duties, that separate functions are performed by separate individuals, and that the concept of least privilege is applied.</p> <p><u>OCPO Comment</u>: OCPO will take steps to ensure that staff are not assigned conflicting duties. However, while we can separate the duties procedurally, the separation cannot be enforced in HPS or SPS without reprogramming. As OCPO anticipates acquiring a replacement system, we will include this capability in the requirements for the replacement system.</p> |
| Page 13 | <p><u>Recommendation 2C</u>: Implement formal policies and procedures to recertify the access granted to users at least an [sic] annually.</p> <p><u>OCPO Comment 1</u>: Delete "an."</p> <p><u>OCPO Comment 2</u>: The OCPO will develop and implement formal procedures for granting access by using the concept of least privilege to OCPO systems, as well as annual user access reviews.</p> <ul style="list-style-type: none"> - Revise system access request forms. - Revise process in which user requests system access. - Revise procedure in which system access is granted. - Develop formal procedure to enforce annual user access review. |

Ref to OIG Evaluation

Auditee Comments

| Comments on OIG's Review of HUD's Procurement Systems | |
|---|--|
| Report Page Reference | OCPO Comments to OIG's Report |
| Comment 12 | <p>Page 13</p> <p>Recommendation 2D: Create and implement routing functionality within the Small Purchase System to allow users to be granted access to more than one office or region.</p> <p>OCPO Comment: OCPO cannot implement routing functionality in SPS without reprogramming. As OCPO anticipates acquiring a replacement system, we will include this capability in the requirements for the replacement system. For the current SPS, OCPO management recommends implementing the following tasks to alleviate the routing issue. OCPO will determine if multiple SPS system profiles are actually a valid requirement on an individual basis. The goal is to eliminate all unnecessary and redundant profiles in SPS.</p> <ul style="list-style-type: none"> • Identify users with multiple HPS profiles • Meet with respective procurement areas to define issue and discuss recommended resolution. • Restructure Issuing Office hierarchy to alleviate the necessity of multiple profiles for a given user. |
| Comment 13 | <p>Page 14</p> <p>Audit Finding 3: For clarity, in the opening paragraph, line 3, we recommend revising "both systems and their" to "either system or in their."</p> |
| Comment 14 | <p>Page 14</p> <p>Audit Finding 3: Interfaces with HUDCAPS Do Not Contain Data Elements to Support Payment and Closeout Processes</p> <p>OCPO Comment: The interface to HUDCAPS was developed to transmit commitment and obligation data from HPS. The data elements required to support payment and closeout process are contained in HUCAPS and other OCFO financial systems. Users are not required to 'exit' from the procurement system to obtain that data from the OCFO's financial system. Required data can be retrieved through either HUDCAPS or the OCFO's Datamart reporting system to obtain the data.</p> |
| Comment 15 | <p>Page 15</p> <p>Audit Finding 3: HUD Did Not Create Interfaces with PAS and LOCCS</p> <p>OCPO Comment: The CFO and CPO offices had begun plans to develop an interface between the HUD procurement systems (HPS/SPS) with the Program Accounting System (PAS). The development cost of the interface was to be funded by the OCFO, however interface development was delayed due to a reprioritization of efforts within the OCFO. An interface with Line of Credit Control System (LOCCS) was never planned within the OCPO.</p> |

Ref to OIG Evaluation

Auditee Comments

Comments on OIG's Review of HUD's Procurement Systems

Comment 16

Comment 17

| Report Page Reference | OCPO Comments to OIG's Report |
|-----------------------|---|
| Page 15 | <p><u>Audit Finding 3</u>: Federal Regulations Mandate Data Elements That Must Exist in the Acquisition and Financial Systems Interface</p> <p><u>OCPO Comment</u>: JFMIP SR-02-02 states that interfaces between financial systems and acquisition systems must exist in the procurement process. However, the interface is not required to be an electronic interface, only that an interface exist in the process. These interfaces do exist in the HUD acquisition process; they are accessed outside the procurement system. The financial details they state as requirements are available electronically as part of the HUD procurement process, just not in an electronic interface format with the HUD procurement systems. OCPO agrees that an electronic interface would improve HUD's ability to manage procurement more efficiently and effectively, and we plan to implement this capability with the replacement system. However, it is not a requirement.</p> |
| Page 16 | <p><u>Audit Finding 3</u>: Acquisition and Financial Systems Must Be Linked to Create a Single Integrated Federal Financial Management System</p> <p><u>OCPO Comment 1</u>: In the heading, change "Federal" to "Agency." OMB Circular A-127, paragraph 6, establishes policy for "[a]n agency's single, integrated financial management system," not a single Federal system.</p> <p><u>OCPO Comment 2</u>: In the body of the paragraph under this heading, beginning in line 2, change "for a single integrated federal financial" to "each agency to have a single financial."</p> |
| | <p><u>OCPO Comment 3</u>: JFMIP SR-02-02 states that interfaces between financial systems and acquisition systems must exist in the procurement process. However, the interface is not required to be an electronic interface, only that an interface exist in the process. These interfaces do exist in the HUD acquisition process; they are accessed outside the procurement system. The financial details that the report states as requirements are available electronically as part of the HUD procurement process, just not in an electronic interface format with the HUD procurement systems. OCPO agrees that an electronic interface would improve HUD's ability to manage procurement more efficiently and effectively, and we plan to implement this capability with the replacement system. However, it is not a requirement.</p> |

Ref to OIG Evaluation

Auditee Comments

| Comments on OIG's Review of HUD's Procurement Systems | |
|---|---|
| Report Page Reference | OCPO Comments to OIG's Report |
| Comment 18 | <p>Page 16</p> <p><u>Audit Finding 3:</u> Financial Data Were Not Incorporated into the Procurement Systems</p> <p><u>OCPO Comment:</u> The interface to HUDCAPS was developed to transmit commitment and obligation data from HPS. The data elements required to support payment and closeout process are contained in HUCAPS and other OCFO financial systems. Users are not required to 'exit' from the procurement system to obtain that data from the OCFO's financial system. Required data can be retrieved through either HUDCAPS or the OCFO's Datamart reporting system to obtain the data. Funds have not been made available to do extensive development work to HPS; OCPO does anticipate replacing HPS/SPS with a commercial-off-the-shelf system to help manage the HUD procurement process.</p> |
| Comment 19 | <p>Page 17</p> <p><u>Audit Finding 3:</u> Conclusion</p> <p><u>OCPO Comment:</u> In line seven of the paragraph insert "record the" before "obligation." Obligation occurs when the contracting officer executes a contract action. The obligation is recorded and processed in the systems.</p> |
| Comment 20 | <p>Page 17</p> <p><u>Audit Recommendation 3A:</u> Perform a cost benefit analysis to determine whether it is more advantageous to modify or replace the procurement systems to ensure compliance with Joint Federal Management Improvement Program Requirements.</p> <p><u>OCPO Comment:</u> OCPO will perform the recommended cost benefit analysis.</p> |
| Comment 21 | <p>Page 17</p> <p><u>Audit Recommendation 3B:</u> Implement functionality to ensure that there is sufficient information within HUD's procurement systems to support the primary acquisition functions of fund certification, obligation, deobligation, payment, and closeout.</p> <p><u>OCPO Comment:</u> OCPO will include such functionality in the requirements for the replacement system.</p> |
| Comment 22 | <p>Page 22</p> <p><u>Audit Finding 4:</u> Participation in the System Certification and Accreditation Process Was Inadequate</p> <p><u>OCPO Comment:</u> The OCPO agrees that the HPS and SPS need improved security documentation. However, the OCPO did work in coordination with the OCIO on the security certification and accreditation efforts, as well as in obtaining OCIO approval to the revised information system categorization.</p> |

Ref to OIG Evaluation

Auditee Comments

Comments on OIG’s Review of HUD’s Procurement Systems

Comment 23

| Report Page Reference | OCPO Comments to OIG’s Report |
|-----------------------|---|
| Page 25 | <p><u>Recommendation 4A:</u> Obtain the training and or resources necessary to develop or perform compliant (1) information system categorization analyses; (2) risk assessments; (3) security plans; (4) contingency plans and tests; (5) monitoring processes, which include applicable Federal Information Processing Standards Publication 200 managerial, operational, and technical information security controls; and (6) evaluations of the managerial, operations, and technical security controls.</p> <p><u>OCPO Comment:</u> OCPO agrees that some security documentation is not current and is undertaking efforts to update the documents to current OCIO requirements. The current HPS/SPS contractor for operations and maintenance may update some of the documentation if funds become available. OCPO will work with OCIO to update other documentation that is outside the scope of that contract. OCPO will also identify and obtain training that will help improve our execution of system security requirements in the future.</p> |
| Page 25 | <p><u>Recommendation 4B:</u> Complete the corrective actions for the known open information security vulnerabilities or develop mitigation strategies if new system development is underway.</p> <p><u>OCPO Comment:</u> OCPO will work with OCIO to develop mitigation strategies for the known open information security vulnerabilities.</p> |
| Page 25 | <p><u>Recommendation 4C:</u> Designate a manager to assume responsibility for ensuring the Office of the Chief Procurement Officer’s compliance with federal certification and accreditation process requirements and to provide “continuous monitoring”: of the office’s information systems security.</p> <p><u>OCPO Comment:</u> OCPO will designate a manager to assume responsibility for compliance with federal certification and accreditation process requirements. It is not practicable or efficient at this time for OCPO to conduct “continuous monitoring” of information systems security as this would assume we have personnel dedicated solely to the function of information security. OCPO will make efforts to better manage the certification and accreditation documentation process as well as other information security documents. However, continuous monitoring and technical aspects of the federal certification and accreditation and information systems security processes will be more efficiently and effectively conducted by HUD’s OCIO. OCIO can centrally acquire the needed resources and skills (in-house or through contract support) to perform this work, avoiding duplicative and underutilized capabilities among individual system owners.</p> |

Comment 24

Comment 25

Ref to OIG Evaluation

Auditee Comments

Comments on OIG's Review of HUD's Procurement Systems

Comment 26

Comment 27

| Report Page Reference | OCPO Comments to OIG's Report |
|-----------------------|--|
| Page 25 | <p><u>Recommendation 4D</u>: Reevaluate the HUD Procurement System and Small Purchase System application systems' security categorization in light of Office of Management and Budget guidance on personally identifiable information.</p> <p><u>OCPO Comment</u>: OCPO will work with OCIO to properly and consistently categorize the systems.</p> |
| Page 25 | <p><u>Recommendation 4E</u>: Perform a business impact analysis for the procurement systems. Based on the results of the impact analysis, determine what actions HUD can take to limit the amount of time needed to recover from the various levels of contingencies that can occur and include the determined actions in the contingency plans for the systems.</p> <p><u>OCPO Comment</u>: OCPO will work with OCIO to perform the business impact analysis.</p> |

OIG Evaluation of Auditee Comments

- Comment 1** OIG disagrees with the Department’s statement that it is not appropriate for HUD’s procurement systems to contain controls that prevent or detect users’ exceeding their procurement authority. The stated purpose of the systems is to provide the Department the information necessary to monitor procurement activities. As noted in the finding, the procurement systems do not currently contain enough information for a person to determine whether the actions taken are appropriate; i.e., the contract officer field is not required. Reports generated from the systems at this time will not provide enough information to allow adequate oversight.
- Comment 2** The Department’s response relates to the input of transactions within the applications. The finding relates to authorization or approval of the transaction. No modifications were made to the finding.
- Comment 3** OIG commends the Department for taking immediate actions in reviewing these transactions. No modifications were made to the finding.
- Comment 4** OIG commends the Department for taking immediate actions in reviewing these transactions. Contract officer review and approval of the data input into the procurement systems will provide HUD with assurance that the procurement action is valid, authorized, and appropriate. No modifications were made to the finding.
- Comment 5** OIG commends the Department for its immediate implementation of this recommendation. Implementation of the remaining recommendations will ensure that these types of reviews are no longer necessary.
- Comments 6, 7** OIG agrees and has added the suggested language to the report.
- Comments 8, 9, 10** OIG is concerned about the Department’s reliance on replacing the system to address the issues cited. A timeframe for replacement of the procurement systems is uncertain. The Department must have an adequate plan in place for the current systems to ensure that controls within the system, or any compensating controls implemented, provide an adequate level of assurance that procurement transactions are accurate, valid, and authorized.
- Comment 11** OIG agrees with the Department’s comment and commends its willingness to make the recommended changes.
- Comment 12** See OIG’s evaluation to comments 8, 9, and 10 above.
- Comment 13** OIG agrees and has made the suggested revision to the report.
- Comment 14** Based on our review, there is no ability to access payment or closeout data within the interfaces between the procurement systems and HUDCAPS. A user can obtain the information from the HUDCAPS system or, if applicable, another system managed by the Office of the Chief Financial Officer, but the user must exit the procurement system and enter those systems separately.

- Comment 15** OIG agrees with the information provided in the Department’s response. The payment information in the Line of Credit Control System would be obtained through its interface with the Program Accounting System. We have clarified the language in the report.
- Comment 16** OIG disagrees with the Department’s comments. The federal requirements of a single integrated financial management system do not require that the acquisition system duplicate or contain the functionality of the payment system; they require that only the acquisition system be able to access the data within the financial system which performs that function. HUD’s acquisition systems do not provide access to the financial data maintained in the Department’s financial systems. Office of Management and Budget Circular A-127 states that financial systems must be linked electronically to be effective and efficient.
- Comment 17** OIG disagrees with the Department’s statement that electronic interfaces between procurement and financial systems are not required. However, we agree with the wording change request and clarified the report.
- Comment 18** OIG disagrees with the Department’s comment. Users are not able to access payment information through the procurement systems’ interface but are required to exit the systems and access others. For example, users have the ability to access payment information from the HUDCAPS application, HUD’s data mart, or other Office of the Chief Financial Officer applications.
- Comments 19, 20** OIG agrees and has made the suggested revision to the report.
- Comment 21** OIG is concerned that the Department’s response is totally reliant upon replacement of the systems. The Office of the Chief Procurement Officer must develop plans to ensure that functionality is included in the current systems and processes in case replacement of the systems does not occur or does not occur soon.
- Comment 22** OIG notes that the Department’s comment is an appropriate step and will review the requirements document when it is available.
- Comments 23, 24** OIG agrees with the Department’s comments.
- Comment 25** OIG disagrees with the comment. The Office of the Chief Procurement Officer did not participate or fulfill its responsibilities in a compliant manner. For example, if the office had fully participated in the certification and accreditation process, the security documents would have been updated at the end of the process.
- Comments 26, 27** OIG agrees with the Department’s comments.