

---

# AUDIT REPORT



PUBLIC AND INDIAN HOUSING INFORMATION CENTER  
(PIC)

PUBLIC AND INDIAN HOUSING

2003-DP-0001

SEPTEMBER 10, 2003

INFORMATION SYSTEMS AUDIT DIVISION  
OFFICE OF AUDIT



Issue Date	September 10, 2003
Audit Case Number	2003-DP-0001

TO: Michael Liu, Assistant Secretary for Public and Indian Housing, P  
Vickers B. Meadows, Assistant Secretary for Administration, A

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

SUBJECT: Audit Report on the Public and Indian Housing Information  
Center (PIC)

We have completed an audit of administrative and technical controls over the security of HUD's Public and Indian Housing Information Center (PIC). PIC is a web-based information system designed to facilitate a more timely and accurate exchange of data between Public Housing Agencies (PHAs) and local HUD offices by allowing PHAs to electronically submit information to HUD. The purpose of our audit was to assess the security of PIC data. Controls over the collection, processing, and reporting of PIC data were not within the scope of this audit.

We found deficiencies and weaknesses in administrative and technical controls over the security of PIC data. The effect of the deficiencies and weaknesses is exposure of PIC data to unnecessary risks of loss of confidentiality, integrity, and availability. In our opinion, there are unnecessary risks of system disruption, exploitation of PIC for identity theft and fraud, and destruction of PIC data by malicious hackers or disgruntled employees. These risks have not been sufficiently diminished by using cost-effective controls.

PIH has taken action to correct several control weaknesses. More remains to be done. In our judgment, the deficiencies and weaknesses we found resulted from inadequate planning for security in the PIC system development life cycle. Consequently, we recommend that PIH now conduct a comprehensive vulnerability and risk assessment, develop a comprehensive security plan for PIC, and correct deficiencies and weaknesses in operational and technical controls as indicated in specific recommendations at the end of this report.

In accordance with HUD Handbook 2000.06 REV-3, within 60 days please provide us, for each recommendation without management decisions, a status report on: (1) the corrective action taken; (2) the proposed corrective action and the date to be completed; or (3) why action is considered unnecessary. Additional status reports are required at 90 days and 120 days after report issuance for any recommendation without a management decision. Also, please furnish us copies of any correspondence or directives issued because of the audit.

We appreciate the courtesies extended to the audit staff. Should you or your staff have any questions, please contact me at (202) 708-0614 extension 8149 or Jay Jacobsen at extension 8137.

Attachment



# Executive Summary

---

We completed an audit of management, operational, and technical controls over the security of HUD's Public and Indian Housing Information Center (PIC). PIC is a technologically advanced web-based information system designed to facilitate a more timely and accurate exchange of data between Public Housing Agencies (PHAs) and local HUD offices by allowing PHAs to electronically submit information to HUD.

We found deficiencies and weaknesses in controls:

- There are inadequate queries and reports for monitoring and controlling user access to PIC.
- A comprehensive process for monitoring and controlling PIC user access is not in place.
- Access controls over the PIC Security Administration Sub-Module are inadequate.
- There is no segregation of duties over the Security System Administration function.
- Controls for safeguarding confidential and sensitive PIC data are inadequate.
- Access controls for identifying and authenticating PIC users are weak.
- System and application audit logs are not being utilized for security and system maintenance purposes.

In our judgment, the deficiencies and weaknesses in controls were caused by inadequate planning for security in the PIC system life cycle. A comprehensive assessment of vulnerabilities and risks was not performed during the initiation or development/acquisition phases of the PIC system life cycle. Furthermore, a comprehensive security policy was not prepared before security aspects of the PIC system were developed.

The effect of the deficiencies and weaknesses in controls is exposure of PIC data to unnecessary risk of loss of confidentiality, integrity, and availability. PIH has taken action to correct several control weaknesses. More remains to be done. In our opinion, there are unnecessary risks of system disruption, exploitation of PIC for identity theft and fraud, and destruction of PIC data by malicious hackers or disgruntled employees. These risks have not been sufficiently diminished by using cost-effective controls.

## **Recommendations**

We recommend that PIH conduct a comprehensive vulnerability and risk assessment, develop a comprehensive security plan for PIC, and correct deficiencies and weaknesses in operational and technical controls as indicated in specific recommendations at the end of this report.

---

# Table of Contents

---

Transmittal Memorandum	i
------------------------	---

---

Executive Summary	iii
-------------------	-----

---

Introduction	1
--------------	---

---

## Finding

Inadequate Security Planning in the System Life Cycle Has Resulted in Significant Security Control Weaknesses in PIC	5
--	---

---

## Appendices

A. Auditee Comments	29
B. Description of Microsoft SQL Server C2 Evaluation	34

---

# Introduction

HUD's Public and Indian Housing Information Center (PIC) is designed to facilitate a more timely and accurate exchange of data between PHAs and local HUD offices by allowing PHAs to electronically submit information to HUD. First released in December 1999, PIC introduced an Internet-based approach that enables PHA users and HUD personnel to access a common database of PHA information via their web browser. Since the inception of PIC, more than 600 transactional web pages have been created; a detailed inventory of 1.3 million public housing units was established; and tenant family data for 3.5 million households was gathered. PIC represents the largest Internet-based system in HUD with over 3.6 million lines of code.

There are approximately 4,000 user logins each day made by over 12,000 authorized HA and HUD users. These users upload over 800 files to PIC daily, with the PIC system processing over thirty thousand Family Reports (form HUD-50058s), which equates to over one million transactions per day.

PIC centralizes information regarding the monitoring and recovery efforts of Housing Authorities undertaken by the field or Troubled Agency Recovery Centers (TARCS). Since PIH's housing inventory data resides in both the PIH Information Center and the Integrated Business System (IBS), it was necessary to migrate the existing IBS Housing Authority functionality into the PIH Information Center to provide a central repository for tracking and maintaining public housing inventory data. HUD PIH users also require a central repository to view Housing Authority characteristics and contact information. PIC enables Housing Authorities to update their data online. This allows field personnel to focus on providing assistance to Housing Authorities and reducing the burden of paper submission and data entry. PIC also enables Local HUD Offices to focus on upholding fair housing practices.

In the future, PIC may support a requirement for PIH to maintain a detailed audit trail of interactions with Housing Authorities and track findings to closure. PIC makes data that is currently in the IBS available to traveling PIH users and business partners through the Internet. This will provide remote HUD users and traveling employees the ability to access PIH systems from their desktops regardless of whether or not they are located within a HUD office.

The PIC systems, modules and Web applications currently in PIH's production environment include:

- PIC Security Maintenance,
- Risk Assessment,
- Housing Authority (HA),
- Housing Authority Development/Demolition Disposition,
- Public Housing Drug Elimination Program (PHDEP) Formula,
- PHDEP Drug Elimination Reporting Subsystem (DERS),
- PHA Development (Building/Unit Inventory),
- Executive Summary; Management Reports,
- Event Tracking System (ETS),
- Section 8 Management Assessment Program (SEMAP),

- Form 50058 (Viewer, Submission, Reports and Alternate ID generator),
- Ad-hoc reports; Security/Database Administration, and
- Office of Native American Programs (Annual Performance Reports – APR).

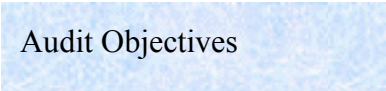

During this audit, we reviewed only the PIC Security Maintenance submodule. We did not review any of the other PIC systems, modules, or web applications.

The Security Maintenance submodule controls user access for more than 12,000 users utilizing three separate databases. It allows PIC Security Administrators to create and maintain users, as well as create and maintain user roles. PIC Security Administrators assign roles to users and determine which user roles have access to the different entities and security levels within the respective system modules.

The PIC technical architecture consists of Microsoft’s Windows 2000 Advanced and Data Center Server, Internet Information Server (IIS) Server 5.0, Microsoft’s COM+ Services, and SQL Server 2000. The application software includes Active Server pages (ASP), JAVA Servlets, COM objects written in Microsoft Visual C++, XML, Java Script, Visual Basic Script, and stored procedures.

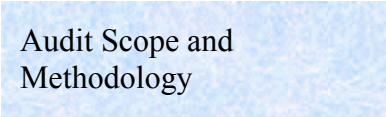
FY 2002 funding for PIC was approximately \$18.8 million and is estimated to be approximately \$26 million for FY 2003, depending on the outcome of pending appropriation requests.

---



Audit Objectives

The initial audit objective was to review selected application controls over the PIH Information Center (PIC) system. Initially, our PIC survey focused on system security access controls as well as controls over data integrity to ensure that data is protected against errors, loss, or unauthorized use. However, due to the complexity of the system and associated issues, our audit objective was changed to reviewing only the system security controls for this audit. At the completion of this audit, we will perform a separate review of data integrity controls to ensure that data is protected against errors, loss, or unauthorized use.



Audit Scope and Methodology

During the survey phase of this audit, we determined that a comprehensive risk assessment was not completed on the PIC system during the early stages of design and development. We concluded that this breakdown during the development process would have the most significant impact on three of the PIC modules: (1) security, (2) Form HUD-50058 (this sub-module collects, stores, and generates reports on families who participate in Public Housing, Indian Housing, or Section 8 rental subsidy



programs), and (3) Section 8 Management Assessment Program (SEMAP). These modules represent major information systems development efforts and also are the most critical to HUD in terms of confidentiality, integrity and availability of data. Due to the complexity of the system, the scope of this audit was limited to the security maintenance submodule. We did not review any of the other PIC systems, modules, or web applications.

Our review of the PIC security module application included analyzing the PIC Security and Navigation databases. Also, we reviewed the PIC infrastructure, which included reviewing the security settings on the Internet Information Server (IIS) web server, Windows 2000 operating system, and SQL 2000 database.

We conducted interviews with various program personnel and obtained documentation on the PIC system design, access controls, and security settings, and also the policies and procedures related to the internal control areas identified above.

We also reviewed criteria, such as:

- HUD Policies and Practices, including application development procedures of the System Development Lifecycle,
- GAO's Federal Information System Controls Audit Manual (FISCAM),
- Federal Information Processing Standards (FIPS) Publication 73,
- NIST guidance, and
- Industry best practices.

We performed analysis and selected testing of the PIC Security and Navigation databases using data mining techniques. In addition, we selected users with security administration rights at the Headquarters, PIH HUB Office Director and Field Office levels to determine whether the PIC application access rights assigned to those users were appropriate.

We reviewed the system access records for nine PHA level users to illustrate known system processing problems within PIC. Specifically, we reviewed users granted access

through the Michigan State Housing Development Authority, Mount Clemens, Traverse City and Saint Clair Shores Housing Commissions to ensure that decentralized security administrators had a proper separation of duties (i.e., there are no indications that users had access to any data or functionality within the system that conflicted with their job functions or their security administration rights). We performed a retrieval of all records within the PIC security database that identified a user as a security administrator. We determined that there are 11,967 records of PIC system administrators in the PIC security database—to perform an analysis of user roles. The analysis was limited to identifying records of security administrators only and does not necessarily reflect the actual number of users with access to the security administration module because some users could be assigned using access multiple roles (the 11,967 amount may represent the same user more than once). Of the 11,967 identified security administrators, we identified 320 different roles available, but only 43 roles were utilized (13 percent of the roles utilized). The roles utilized the most were numbers 9 (access without the ability to create roles), 239 (view user activity) and 1 (all functionality except create templates). During this analysis we reviewed the activity of the PIC Security Administrator and determined that he was also performing System Administrator functions, which violates the principle of segregation of duties.

We performed our audit work at HUD Headquarters and at the HUD Detroit Field Office. The audit covered the period from November 2002 through February 2003.

The audit was conducted in accordance with generally accepted government auditing standards. Accordingly, we included such tests and other auditing procedures that we considered necessary under the circumstances.

We provided a copy of this report to the Assistant Secretary for Public and Indian Housing.

---

# Inadequate Security Planning in the System Life Cycle Has Resulted in Significant Security Control Weaknesses in PIC

We found that security planning in the system life cycle for the PIC system was inadequate. Comprehensive system sensitivity and risk assessments were not performed in the initiation and development/acquisition phases of the system life cycle. Additionally, we found that a comprehensive security policy and goals were not prepared in formulating the design of the security aspects of the PIC system. As a result, several operational and technical security control weaknesses were found during the audit. Specifically, we found (1) inadequate PIC system design structure and documentation has impeded PIH's ability to monitor and control users' computer access, (2) no comprehensive process has been established to monitor and control PIC user access, (3) access controls over the Security Administration sub-module are not adequate, (4) separation of duties are needed over the System Administration function, (5) inadequate controls exist over confidential and sensitive PIC data, (6) access controls need to be strengthened to identify and authenticate users to the PIC application and database, and (7) system and application audit logs are not being utilized for security and system maintenance purposes. Without adequate security controls over the PIC system, HUD is at risk that data errors and omissions and system disruptions could occur, and that the system could be exploited by unauthorized individuals for fraud and identity theft as well as the potential for destruction of data by malicious hackers and disgruntled employees.

---

## Background

The PIC technical infrastructure is based on a 3 tier architecture. The first tier comprises a series of border routers and firewalls to isolate the second and third tiers against unauthorized access and intrusion. The second tier comprises the business logic which is located on a web farm consisting of a cluster of eight web servers. The servers all run Microsoft's Internet Information Server (IIS) and COM+ applications. Each server in the web farm is also configured with a Microsoft Windows 2000 Advance Server network operating system. The web servers determine what data is needed, where it is located, and acts as a client in relation to a third tier. Business and application data is stored in the production SQL database residing on the third tier server. The SQL database is configured with a Microsoft Windows 2000 DataCenter Server operating system.

The PIC system is constructed of six integrated, yet distinct, layers that make up the fabric of the PIC Application Architecture: the Business Layer, the Services Layer, the Security Layer, the Data Layer, the Development Layer and the Operations Layer. The Security Maintenance sub-module in PIC is part of the Business Layer and allows PIC Security Administrators the ability to create and maintain users, as well as create and maintain roles. This sub-module controls access to the PIC data for the approximately 12,000 internal and external PIC users.

### **Comprehensive Security Sensitivity and Risk Assessments were not Performed**

#### **Criteria**

NIST Special Publication (SP) 800-12, An Introduction to Computer Security, The NIST Handbook, Chapter 8 provides that basic security aspects of a system should be developed along with the early system design in the initiation phase of the system life cycle. This can be done through a sensitivity assessment. The sensitivity assessment starts an analysis of security that continues throughout the system life cycle. A sensitivity assessment looks at the sensitivity of the information to be processed and the system itself. Sensitivity is normally expressed in terms of integrity, availability, and confidentiality. This assessment is used to determine what security controls should be incorporated in the design of the system to prevent unauthorized modification and disclosure, or unavailability of the system or data.

Chapters 7 and 8 of NIST SP 800-12, discusses computer security risk management and how a risk assessment is critical in identifying and mitigating security vulnerabilities by implementing cost-effective controls and safeguards throughout the system life cycle. A primary function of computer security risk management is the identification of appropriate controls. Risk should normally be assessed during the requirements analysis phase or design phase of a system developments cycle. Risk should also normally be assessed during the development/acquisition phase of a system upgrade.

We found there was no evidence that comprehensive security sensitivity and risk assessments were performed to evaluate the assets, threats, and vulnerabilities of the system

to determining the most appropriate, cost-effective safeguards and controls.

**Comprehensive Security Policy and Goals were not Prepared in the Formulation of the PIC System Security Design**

**Criteria**

NIST SP 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), provides a list of system level security principles to be considered in the design, development, and operation of an information system. Principle 1 is to establish a sound security policy as the “foundation” for the design. The security policy begins with the organization’s basic commitment to information security formulated as a general policy statement. The policy is then applied to all aspects of the system design or security solution. The policy identifies security goals (e.g. confidentiality, integrity, availability, accountability, and assurance) the system should support, and these goals guide the procedures, standards, and controls used in the IT security architecture design. The policy should also require definition of critical assets, the perceived threat, and security related roles and responsibilities.

Based on our review of the PIC system documentation provided, we found that PIH did not establish a comprehensive system security policy that defined the critical assets, the perceived threat, and the security related roles and responsibilities which would form the basis for the security design of the PIC system. Additionally, security goals based on this policy were not established.

**Current system documentation does not identify security procedures, standards and controls that were considered in the PIC security design structure**

PIH has developed System Architecture and System Administration Guide documents. However, although security aspects were apparently considered in the formulation of these documents, the documents did not identify the security procedures, standards or controls that were considered in the design of the PIC system which could be traced and linked to the security goals and to an overall PIC security policy. For example, the System Architecture document provides a high-level review of the technical infrastructure and application architecture based on PIH business objectives. The document discussed, in part, the “Security Layer” for PIC which comprises a set of services and controls that facilitate User Profile Management,

Logon/Session Management, User Access/Navigation and Data Access. However, the document only provided a high-level view of the control structure for access to PIC data and did not define the specific rules and procedures that should be applied based on a particular control and standard or that could be traced to a specific goal and the security policy.

**Weak security controls places HUD at risk for unauthorized access and disruption to PIC system and errors or omissions of critical PIC data**

The lack of comprehensive security sensitivity and risk assessments and system security policy and goals has resulted in our identification of several significant security control weaknesses in the PIC system. We found (1) inadequate PIC system design structure and documentation has impeded PIH's ability to monitor and control users computer access, (2) no comprehensive process has been established to monitor and control PIC user access, (3) access controls over the Security Administration sub-module are not adequate, (4) separation of duties are needed over the System Administration function, (5) inadequate controls exist over confidential and sensitive PIC data, (6) access controls need to be strengthened to identify and authenticate users to the PIC application and database, and (7) system and application audit logs are not being utilized for security and system maintenance purposes. Without adequate security controls over the PIC system, HUD is at risk that data errors and omissions and system disruptions could occur, and that the system could be exploited by unauthorized individuals for fraud and identity theft as well as the potential for destruction of data by malicious hackers and disgruntled employees. PIH management agreed that comprehensive sensitivity and risk assessments were not performed and stated that they are currently in process of engaging a contractor to develop these assessments. The security control weaknesses identified during our review are discussed in more detail in the following paragraphs.

#### **Inadequate Queries and Reports for Monitoring and Controlling User Access to PIC.**

**Security Design Background**

The security layer utilizes three databases in PIC to control access to PIC data, the PIC DB, the PIC Navigation DB and the PIC Security DB. The PIC DB is the main application database, all the module specific information is stored in this database. The PIC Security database provides role-based access to the application data using data access hierarchies. The PIC Navigation database provides the mechanism to allow a user to navigate application data hierarchies in the

PIC database. These databases contain tables that provide the application security for the PIC system. The PIC security application architecture utilizes Data Access Containers (Containers). A container is a data element such as a person, an event, or an office that define relationships to facilitate data access in the system. Containers define the rules of data relationships to mirror the HUD organizational structure. A role is defined to represent a set of tasks or privileges that a user may perform; it cannot apply to more than one module. When application functionality is retrieved in PIC, the user's role and data access are used to create the web page (screen). The sub-modules, business functions, page groups, actions, and data are all retrieved based upon the users' privileges.

As part of our audit procedures, the specific access levels of twelve users (three HUD, eight PHA and one PHA vendor) were traced through the security screens and database tables to illustrate the process and to determine whether the users had proper access entitlements/privileges corresponding to their duties and responsibilities. However, we were unable to verify whether the users had the appropriate access because (1) user access roles and relationships within the PIC security design were not adequately defined and documented, and (2) the PIC Security Maintenance sub-module lacks the queries and reports necessary to identify the total access granted to users.

**PIC user access roles and relationships were not adequately defined and documented**

When a user makes a data request, the user's access to business transactions is dependent on the roles assigned to the user for the data and the current relationships defined in the containers. However, we found that user roles could not be traced to the specific data elements. Additionally, the hierarchy and the parent child container relationships within the application are not clearly defined.

Although we were provided documentation on the PIC system architecture, the documentation only provided general descriptions of PIC roles and relationships. The documentation lacked sufficient details on the access provided by the roles and the relationships of specific data elements to each other. Without these details we could not determine how these relationships are combined and linked to specific screen presentations. As a result, we could not determine whether users had the proper

entitlements/privileges based on their duties and responsibilities.

**Current PIC security screens are inadequate for determining total users with access to a specific organization's data**

Our review also found that the security screens are inadequate to determine the total users who have access to a particular organization's data. The access information on the security screens for a particular user is based on the organization the user's primary access was granted under although the user may have access to other organizations data. A user that is not specifically granted access to a particular organization as their primary access will not show up in the system as having access to other organizations. Accordingly, to determine the access granted to a specific organization, such as a PHA, an individual responsible for monitoring and controlling user access, e.g. security administrator, would need to know either all the users within all of the various organizations that have access to the data or would need to know all of the organizations that have access to the data and search for users with access to the data.

For example, we identified a vendor employee with access to 80 different PHAs under their access granted to their primary PHA. However, when we reviewed the PIC security screens for four of the 80 PHAs listed under their primary access, we found that the vendor is not listed on the PIC system security administration screens as having access to the data for these entities. Consequently, a person, such as a Security Administrator responsible for reviewing security data for a PHA, would be unable to determine the complete level of access the vendor has without specific knowledge of (1) who has access to this data, or (2) every organization that has or could have access and then trace the individuals within the organization to determine if they have access, a very complex and time consuming process.

**PIH does not have a means to readily identify the number of PIC users with data access rights identifiable to a specific PHA**

When we brought this condition to PIH management's attention, they agreed that the current system design does not provide the capability to identify the total access granted to a particular organization but could be done through writing queries to the PIC database using the Structured Query Language (SQL) tool. We requested that PIH provide us the total number of PIC system users with data access rights identifiable to a specific PHA. However, because of the complexity and time involved in writing these queries, it



was determined that this information would not be available within the remaining audit timeframes.

Without adequate documentation that defines the access roles and relationships and the ability of the PIC security system to identify the total users who have access to a particular organization's data, PIH has no means to properly monitor and control users access to critical and sensitive PIC data.

**PIH Has Not Established a Comprehensive Process to Monitor and Control PIC User Access.**

**Criteria**

NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, states that organizations should ensure effective administration of user's computer access to maintain system security. Organizations should have a process for 1) requesting, establishing, issuing, and closing user accounts, 2) tracking users and their respective access authorizations, and 3) managing these functions. In addition, the guidance states that it is necessary to periodically review the levels of access each individual has, conformity with least privilege, whether all accounts are still active, whether management authorizations are up to date, etc. Additionally, an organization should consider both internal and external access control mechanisms. Internal access controls are a logical means of separating what defined users (or user groups) can or cannot do with system resources. External access controls are a means of controlling interactions between the system and outside people, systems, and services. One of the access control mechanisms that can be used is the access control lists (ACL's). ACL's are a register of users (including groups, machines, processes) who have been given permission to use a particular system resource and the types of access they have been permitted.

**No comprehensive process or control mechanism exists to periodically review users access to critical and sensitive PIC data**

PIH did not have a process to periodically review the levels of access for each individual, whether the access the user has conforms with the principle of least privilege, and whether all accounts are still active and management authorizations are up to date, etc. Although, PIH has established a Security Administrator function within PIC, there was no requirement for the Security Administrator to maintain records or obtain management authorizations to support user

access. We also found access control lists were not being maintained that identified all PIC system users and the type of access they were given. Additionally, no re-certification process is in place to ensure that users are only granted access to those rights and privileges necessary to perform their official duties. Lastly, although PIH has developed a System Administrator Guide (Guide), we found that the Guide lacked comprehensive system specific security policies, procedures, or guidelines for monitoring the system security access for both internal and external PIC users to conform to NIST guidelines.

It is critical that a comprehensive process and control mechanism be established for periodically reviewing users access. A re-certification process, along with access control lists, will ensure that only authorized users have access to critical and sensitive PIC data commensurate with their duties and responsibilities.

#### **Access Controls Over the Security Administration function Are Not Adequate**

#### **Criteria and background**

HUD Handbook 2400.24 (Chapter 4, Section 2 part b), refers to requirements in the Computer Security Act of 1987 and OMB A-130 that require that program managers be responsible for determining who, and at what level staff should have access to major application systems. Chapter 5 Section 9 part A states that:

*"System Owners also must determine the level of access required. The levels of access are the rights and privileges held by the individual for an information system. Access approval is based on the principles of need-to-know and least privilege. Need-to-know is determined by the individual's verified need to access information for a particular job function. The principle of least privilege ensures that users will only have the minimum privileges needed to carry out their duties."*

NIST SP 800-14 Paragraph 3.12. 1 provides that organizations should control access to resources based on access criteria. One access criteria is the use of roles. Roles are used to control access by job assignment or function of the user who is seeking access. The process of defining roles should be based on a thorough analysis of how an organization operates and should include input from a wide spectrum of users in an organization.

**Decentralization of Security Administration function to the PHAs and their vendors poses significant risks to PIH's critical and sensitive data**

The PIC Security Administration function is decentralized with security administration rights given to various individuals at HUD Headquarters, the HUD Regional Offices and the Public and Indian Housing Authorities (PHAs). These individuals can, in turn, grant these same or lesser rights to other individuals. The Security Administrator sub-module controls user access rights to PIC. This is a powerful sub-module that allows individuals with access the ability to add, create, or modify users access in PIC.

We performed a retrieval of all records from the user data access table within the PIC security database to identify those users who had access to the Security Administrator sub-module. The analysis was limited to identifying records of access to the Security Administration sub-module only. It does not necessarily reflect the actual number of users with access to this submodule, which would be less, as some users are assigned multiple access types and/or access to multiple locations.

**Security Administration rights were given to PHAs and their vendors without proper oversight and which is contrary to HUD's security policy**

We found that Security Administration rights were granted to Public Housing Authorities (PHAs). In addition, we found four PHA vendors that were granted Security Administration rights by their respective PHAs. These actions are contrary to HUD security policy that System Owners (e.g. PIH) are responsible to determine the level of access required for their applicable system. We also found that PIH did not have proper oversight of the PHAs and their vendors who were given Security Administration rights. PIH did not establish policies and procedures or guidelines to the PHAs detailing whom they could assign access to and the levels of access that could be assigned. In addition, PIH could not monitor the access levels granted to these external organizations because of a lack of functionality in the PIC system that was discussed previously.

PIH, as the system owner, is responsible for the data residing in PIC. Accordingly, PIH needs to have control over the access to the Security Administration function and sub-module by limiting System Administrator rights to HUD personnel only. Allowing external users access to this powerful function increases the risk that errors, omissions

and unauthorized use of critical and sensitive PIC data could occur.

**Controls are needed over the creation and assignment of roles within the Security Administration sub-module**

We found that there were inadequate controls over the creation and assignment of roles within the system. A significant number of roles created and assigned within the Security Administration sub-module were not being utilized. Also, some roles appear to be duplicative while others lacked role descriptions.

At the time of our review, we found 11,967 records that defined user access to the PIC Security Administration sub-module. Of the 11,967 records, we identified 320 different roles that were created and assigned within the sub-module. However, only 43 roles (13 percent) were being utilized. Also, of the 43 roles assigned, three roles (numbers 1, 9, and 239) were utilized 83 percent of the time. We also found roles that lacked a description to determine what the role was created for. For example, we found two roles with the role name of “test” and 14 roles with a role name of “Superuser” that did not contain a role description. Additionally, we found roles that appear duplicative. We identified five different roles with the same description. Roles numbers 74, 127, 145, 152, and 225 were all defined as SEMAP submissions.

Controls over the creation and assignment of roles in PIC are critical to ensure the integrity and availability of PIC data and to prevent confidential information from being disclosed to unauthorized individuals.

**Separation of Duties is Needed Over the System Administration Function.**

**Criteria**

NIST SP 800-14 states that 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. GAO FISCAM 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 polices and organizational divisions. The GAO FISCAM Chapter 3 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 (Security Administrator) function is responsible for developing security policies, procedures, and guidelines and the adequacy of access controls and service continuity procedures. The Data Administration (System Administrator) 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.

**HUD Security Administrators have ability to submit Form HUD-50058 data that should be limited to Housing Authority staff only**

As part of our review, we analyzed the access authority given to three HUD employees assigned the Security Administration role to determine if there was a proper separation of duties. The security administrator is responsible for ensuring that only authorized users have access to the PIC system, which includes coordinating and processing user-ID requests. Accordingly, to maintain a proper segregation of duties, the security administrator should not have the ability to perform a function that is not within their scope of duties or change or delete PIC data.

We found that, because of the way PIC security was designed, all three HUD security administrators have the ability to submit Form HUD-50058 data for processing. The ability to submit Form HUD-50058 data for processing should be limited to Housing Authority staff and is not a function of a HUD user, or within the scope of duties for these users. The current PIC security design requires the security administrators to have all of the access rights and privileges to the resources that they will assign. In order for the HUD security administrators to grant rights and privileges that are inherent housing authority responsibilities such as the processing of Form HUD-50058 data, they must have the same access rights and privileges. Because of this security design weakness, controls are needed to ensure that a proper segregation of duties is established in the security administration function.

**Security and System Administration functions are not properly segregated**

We also found that the PIC Security Administrator, who is responsible for the overall PIC system data security, was also performing data corrections in PIC. In addition to his duties for controlling access to the PIC data, the Security Administrator also has read and write privileges to the PIC database on the SQL 2000 server to fix data errors. The Security Administrator utilizes this access to process data correction SQL scripts written by a HUD contractor. To ensure a proper segregation of duties, these duties represent job functions that should be completed by a System Administrator.

**Security Administration functions of account setup and authorization should be separated**

We determined that the PIC Security Administrator controls both the account setup and authorization process. These functions should be split up so that there is a proper segregation of duties. For example, a possible alternative would be for the OCIO's office to manage account setup, while PIH manages the authorization process.

**Roles and responsibilities for the PIC functions have not been defined to ensure the proper segregation of duties**

PIH has not performed a review of the roles and responsibilities and functions assigned to the PIC system to determine if duties are appropriately segregated. Additionally, PIH has not established policies and procedures that describe the roles and responsibilities and functions to ensure the proper segregation of duties for users performing these functions. For example, we found that, although PIH has prepared a System Administration Guide (Guide) that describes the roles and responsibilities for the System Administrator, there was no documentation to describe the roles and responsibilities for the Security Administrator. Also, we found that the roles and responsibilities described for the System Administration function included roles and responsibilities that should only be assigned to the Security Administration function. For example, one of the responsibilities of the System Administrator identified in the Guide is to assist the security administration function by providing day-to-day account management, i.e. user and group account administration. This responsibility should be assigned to the Security Administrator rather than the System Administrator to ensure the proper segregation of duties.

Inadequately segregated duties increases the risk that erroneous or fraudulent transactions could be processed, that improper program changes could be implemented, and that computer resources could be damaged or destroyed. The Security and System Administration functions should be separated. PIH needs to review the functions within PIC and establish policies and procedures that identify the roles and responsibilities for all of the applicable functions to ensure that the duties are properly segregated. PIH management agreed that the PIC Security Administrator functions will need to be separated from the PIC System Administration functions.

### **Inadequate Controls Exist Over Confidential and Sensitive PIC Data**

#### **Criteria and background**

NIST SP 800-14 defines the key term “confidentiality” as a requirement that private or confidential information not be disclosed to unauthorized individuals. The Computer Security Act of 1987 defines “sensitive” information as any information, the loss, or misuse or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs or the privacy in which individuals are entitled to under the Privacy Act of 1974. The Privacy Act of 1974 states that agencies are required to establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual for whom information is maintained. NIST SP 800-14 Chapter 7 “Computer Security Risk Management” provides that when performing a security risk assessment of a computer system, management should perform an assessment of the consequences from the degree of harm or loss that could occur particularly the significant long term impacts such as from violation of privacy.

Our audit included reviewing the PIC system to determine whether there were adequate controls over confidential and sensitive information. We found that there are several confidential and sensitive data fields in the PIC system that potentially could be seen or printed by unauthorized users or users whose job functions do not require knowledge of the

privacy data to perform their duties. For example, the PIC screens for the Form HUD-50058 Viewer as well as the MTCS sub-module under Ad-Hoc Reports contain confidential and sensitive information on PHA tenants and residents' social security numbers and dates of birth.

**PIH has not performed a risk assessment to identify the impact of potential privacy violations**

Although PIH has identified sensitive data fields that require special provision to restrict read access, PIH has not performed a risk assessment of the consequences to the computer system from the degree of harm or loss that could occur from privacy violations. Currently, there is a risk that confidential information in the PIC system could be compromised. In order to decrease this risk, PIH should (1) identify the various user functions that require access to PIC sensitive data for the user job function, (2) identify the best alternatives to provide the necessary security to those who require access, and (3) establish a mechanism to monitor users' access to the sensitive data. As we have discussed previously in this audit finding, this mechanism should be based on PIH establishing a comprehensive policy and procedures for granting access to both HUD PIC users and external PIC users outside the HUD organization using predefined roles with access levels determined and approved by HUD management. PIH management agreed that policy and procedures should be developed and implemented to protect the confidentiality and sensitivity of PIC data.

Without adequate controls over confidential and sensitive information, such as Social Security Numbers and date of birth of residents and tenants, HUD is at increased risk that this information can be compromised by unauthorized users.

#### **Access Controls Need to be Strengthened to Identify and Authenticate Internal and External Users to the PIC Application and Database**

**Criteria**

NIST SP 800-14 states that Identification and Authentication is a critical building block of computer security since it is the basis for most types of access control and for establishing user accountability. Identification and Authentication is a technical measure that prevents unauthorized people or processes from entering an IT system. Access control usually requires that the system be able to identify and differentiate among users. User accountability requires the linking of activities on an IT



system to specific individuals and, therefore, requires the system to identify users. Identification is the means by which a user provides a claimed identity to the system. The most common form of identification is the user ID. Authentication is the means of establishing the validity of this claim. Passwords are used to authenticate a user's identity. There are several Federal publications/manuals, internal HUD Handbooks, and Industry Best Practices that provide policies and guidelines for establishing access controls over an organization's computer resources.

**Passwords and IDs did not conform to HUD and Federal policies and guidelines, or industry accepted best practices**

Access to PIC resources (i.e. Identification and Authentication) by HUD and external users is controlled through the PIC Security Maintenance sub-module. A review of the access controls for this sub-module disclosed that PIH did not follow HUD and Federal policies and guidelines, or industry accepted best practices on establishing, controlling, and maintaining user passwords and IDs. Specifically, we found:

- Passwords in the PIC system are only required to be five characters in length rather than the current industry best practices standard of 8 characters. Increasing the length of passwords helps prevent guessing of passwords.
- Passwords were not specified and required to contain special characters, not being in an online dictionary, and unrelated to the user ID as recommended by NIST SP 800-14. Requiring passwords to use special characters, not be in an online dictionary, and unrelated to the user ID makes it more difficult for an unauthorized individual or hacker to compromise a users password.
- Passwords were specified to expire every 60 days which is contrary to HUD's policy (HUD Handbook 2400.24) of 21 days. Requiring passwords to be changed every 21 days can reduce the damage done by stolen passwords and can make attempts by an unauthorized individual or hacker to obtain a user's password more difficult.
- Passwords are not made inactive after three unsuccessful login attempts as recommended by

NIST SP 800-44. This restricts an unauthorized user's ability to use password cracking software in attempting to gain access to the system.

- Password history file is not maintained and utilized to ensure that names, words, or old passwords (24 generations) are not reused as recommended by industry accepted best practices and NIST SP 800-12.
- Inactive user IDs are not removed from the system after 6 months as required under HUD Handbook 2400.24. Although PIC user IDs cannot be removed from the system once established, the user IDs can be permanently disabled after 6 months to prevent their use by intruders or any other unauthorized individuals.
- Vendors were given organization IDs rather than IDs assigned to individuals. This restricts individual accountability by making it difficult to trace the actions made by an individual.

Failure to control the confidentiality of passwords and IDs exposes HUD to the risk that unauthorized users may have access to critical and sensitive PIC data resulting in errors, loss, or compromise of the data.

**SQL database server access controls need to be strengthened for identifying and authenticating internal support users**

We also found similar access control problems over the SQL Server 2000. Currently, there are two separate logons required to access the SQL Server 2000 database. PIH uses SQL Server 2000 for data management which is operated on the Windows 2000 Server. The Windows 2000 operating system has its own ID and password which provides the initial access control to the PIC domain. Internal support for the SQL Server 2000 requires that individuals also be assigned a SQL Server 2000 ID in order to perform application and system level database functions such as database software upgrades, backup and recovery monitoring, performance tuning, size planning, and management of the database and related objects.

Our review found several identification and authentication weaknesses that resulted from inherent access control deficiencies within the SQL Server 2000. Password

construction and login security controls were not built in the SQL database server by the vendor. As a result, the SQL Server 2000 allows for a user ID to be used that has no password. In addition, the SQL Server 2000 system parameters do not enforce a password change frequency and locking of an ID after a series of invalid login attempts. However, the Windows 2000 operating system has security features that require IDs to have passwords, enforces password change frequency and provides the capability for locking an ID after a series of invalid login attempts.

**Use of Mixed Mode will provide better control over access to the PIC domain and database**

Under the current security access configuration of the SQL Server 2000, unauthorized takeover of SQL Server 2000 IDs can occur by individuals with access to the Windows 2000 operating system IDs. This can occur by an individual logging on to the Windows 2000 operating system and then performing an additional logon to the SQL Server 2000 to perform SQL functionality. However, this approach does not ensure the owner of the SQL Server 2000 ID is the same as the Windows 2000 ID. Currently, the SQL Server 2000 is operating under the "Standard Security" mode which supports this two level logon (i.e. Windows 2000 and SQL Server 2000 logons). However, the SQL Server 2000 provides the capability to operate under the "Mixed Mode" which combines the SQL Server 2000 and Windows 2000 IDs using Windows 2000 robust access controls.

PIH management agreed with our assessment of the control weakness and will explore the feasibility of implementing the Mixed Mode security option within SQL Server 2000. Without the proper access controls over the PIC SQL Server 2000 database, the confidentiality, integrity, and availability of PIC data is at risk.

### **System and Application Audit Logs are not Being Utilized for Security and System Maintenance Purposes**

**Criteria and Background**

Principle number 20 in NIST SP 800-27 dated June 2001 states that audit mechanisms to detect unauthorized use and to support incident investigations should be implemented. It further states that organizations should monitor, record and periodically review audit logs to identify unauthorized use and to ensure that system resources are functioning properly. NIST SP 800-12 provides that event-based logs can be used

as audit trails for a system. Event based logs usually contain records describing system events, application events, or user events. System audit records are generally used to monitor and fine-tune performance. Application audit trails may be used to discern flaws in applications, or violations of security policy committed within an application. In general, application-level audit trails monitor and log user activities, including data files opened and closed, specific actions, such as reading, editing, and deleting records or fields, and printing reports. A user audit trail monitors and logs user activity in a system or application by recording events initiated by the user (e.g. access of a file, record, or field, use of a modem).

According to the PIC System Architecture document the PIC system has the capability to capture security related event origination details for all transactions. The transaction log records user profile information including the user ID and all transactions or user actions that result in the creation, modification, or deletion of existing application, navigation, or security data. The HUD business dictates the actions that trigger (enable) event logging and the specific data elements that are to be recorded. The PIC Event Log Database is the system event log database that is a repository for event triggered auditing or application logging of the main application database.

Our audit procedures included reviewing the audit logs in PIC to determine whether (1) an audit trail exists which identifies user IDs that have been created and deleted, (2) information regarding additions, changes, deletions to access entitlements is maintained, and (3) they are being used by PIH to monitor security violations and system performance problems. Our review found that PIH management is not using the logging capability in PIC to detect security violations or performance problems.

**PIC application audit log is not currently configured to identify the user to the transaction data recorded**

We found that the PIC application provides a PIC event log that records certain events made by system users. A review was made of the PIC event log on January 23, 2003 to determine the nature and extent of the events that were logged. We found that although the PIC event log recorded transactions made by users, the transactions could not be identified to a specific user. The event log identifies the specific transaction made, the associated database, table, and

column names that the transaction affected, the transaction type code (e.g. update, delete) and the old and new values of the modified record. However, there was no user ID identified which would provide an audit trail of who actually made the transaction.

Audit logs should be used to review what occurred after an event and for periodic reviews to identify unusual activity. Additionally, the review of the audit logs should be made by other than security and/or administration personnel who maintain logical access functions. When we discussed this issue with PIH management, we were informed that the application event log is reviewed primarily when problems occur and that they do not monitor the log on a periodic or real time basis. Additionally, PIH indicated that they do not have any policies and procedures for reviewing this log.

**SQL database server login security and system events are not being fully logged and periodically reviewed**

The SQL Server 2000 is used by HUD as the database for the PIC application. The SQL Server 2000 provides the capability to log security and system events such as changes to server access permissions and backup/restores to system data.

We found that the current security settings to monitor login access events were not adequate. The SQL Server 2000 has four Audit Level security settings; None, Failure, Success, and All. HUD currently has the SQL Server 2000 Audit Level setting to log failed security access attempts only and did not consider adding the capability to log successful attempts. Monitoring successful login attempts can identify whether users are making unauthorized changes to the system. Additionally, we found that PIH was not periodically reviewing the log of failed attempts to effectively detect intrusion attempts by unauthorized individuals.

**PIH needs to use their updated version of the SQL Server 2000 audit log function to provide a more robust and comprehensive audit capability**

We also found that PIH is not using a more robust and comprehensive audit function under the current release of SQL Server 2000 for monitoring PIC security and system performance requirements and events. The new audit function version in SQL Server 2000 has the capability to audit 19 different security and system events such as login/logout, password change event, add/remove database user and role member, derived permissions as well as

backup/restore event, and server shutdown/pause/start. The newer audit function version also has a C2 auditing mode feature that will audit all 19 events. However, we noted that the 19 critical security and system events, to include the C2 auditing mode, were not enabled in the system to log any of these 19 events as PIH was using the older version of the audit function instead. For additional details on the Microsoft SQL Server C2 Evaluation (which describes the criteria used for the C2 auditing mode), refer to Appendix C.

**Policies and procedures for establishing, monitoring and periodically reviewing audit logs have not been established**

PIH has not established policies and procedures requiring the review of audit logs to include how often they should be reviewed, by whom, and specifying the data to be reviewed. The lack of monitoring and maintaining the application audit logs to detect security violations and performance problems places HUD at risk that the confidentiality, integrity, and availability of critical and sensitive PIC data could be compromised.

---

## Auditee Comments

The Assistant Secretary for Public and Indian Housing (PIH) provided a written response to our draft audit report on August 5, 2003. A summary of PIH comments is provided below. PIH's full response to our draft report is included in Appendix A.

PIH agrees that it needs to take steps to enhance the security in the PIC system further. PIH also acknowledged that it did not go through a documented, rigorous analysis of the security required prior to developing the PIC system but rather went through an informal process that adopted existing security models with inadequate analysis of the potential risk. PIH therefore agreed with most of the recommendations in the draft report. Where PIH disagreed, the disagreements primarily related to the specific parameters proposed in a given recommendation rather than the need to have parameters.

---



---

## OIG Evaluation of Auditee Comments

PIH fully agreed with 9 of our 12 draft recommendations. These were recommendation numbers 1A, 1B, 1C, 1E, 1G, 1H, 1J, 1K, and 1L. PIH agreed in principle with the 3 remaining draft Recommendations (1D, 1F, and 1I) but wanted to explore alternative approaches.

In PIH's response to draft recommendation number 1I, PIH agreed with the need to strengthen identification and authentication controls but believes that the specific parameters recommended would not be appropriate in some instances. The specific parameters in our draft recommendation were:

- 21 day password expirations,
- passwords made inactive after three unsuccessful logins,
- 24 generations of passwords not be reused, and
- user identifications be permanently disabled after six months of inactivity.

We concur with PIH on the 21-day password expiration policy, which had been HUD's policy. HUD is now in the process of changing its password expiration policy from 21 to 60 days. Accordingly, we revised draft Recommendation 1I to recommend that passwords be set to expire every 60 days or less.

We also revised draft Recommendation 1I to delete reference to 24 generations of passwords. Nonetheless, we continue to recommend that HUD ensure that previously used passwords are not used again.

We also revised draft Recommendation 1I to delete the term "permanently". We continue to recommend that user accounts or IDs be disabled after six months of inactivity. But we have no objection to reinstatement of disabled user accounts when the user again needs access to the system. However, disabled inactive accounts should not be maintained indefinitely. We recommend liquidation of user accounts that have been inactive for a period of 12 months –

if not sooner – due to a change in the employee’s duties or termination of employment.

Our revised recommendations follow.

---

## Recommendations

We recommend that the Assistant Secretary for Public and Indian Housing (PIH):

- 1A. Conduct a comprehensive security review of the PIC system. This review should include conducting sensitivity and risk assessments and formulating comprehensive security policy and goals. This security review should be used to form the basis for developing comprehensive security policies and procedures, security standards, and controls to ensure that PIC system critical data and resources are adequately safeguarded against waste, fraud, or abuse.
- 1B. Conduct a review of the roles and responsibilities and access rights based on the business rules and the sensitivity of the data. From this review, build SQL queries based on the security logic design to establish a process to monitor user’s access.
- 1C. Remove the application Security Administration function from the PHAs and the vendors and assign it to HUD personnel only.
- 1D. Establish a comprehensive process for monitoring and validating, on a semi-annual basis, users’ access to the PIC system. This re-certification process should include developing policies and procedures that include (a) developing access control lists of users (including groups, machines, processes), (b) how access to the system should be requested, granted and what information should be obtained and maintained on users, (c) limiting access granted to users outside the HUD organization to predefined roles with access levels determined and approved by HUD staff, and (d)



---

specifics regarding who can be assigned security administration rights within the system and how this access will be monitored.

- 1E. Ensure controls are in place for the creation and assignment of roles in the Security Administration sub-module. Additionally, roles in the Security Administration sub-module that are not utilized or are duplicative should be removed. Also, roles should be fully described to determine what they were created for.
- 1F. Perform a review of the roles and responsibilities of PIC users and establish policies and procedures that identifies and defines global roles within the PIC system that maintain a proper segregation of duties to include (a) ensuring HUD security administrators do not have the ability to submit Form HUD-50058 data, and (b) creating separate global System and Security Administration roles within the PIC organization that divides responsibility for data correction and system security functions.
- 1G. Establish system specific policies and procedures for maintaining and controlling the confidentiality of user passwords and IDs.
- 1H. Establish policies, procedures and standards for reviewing audit logs. The audit logs should be reviewed by personnel other than security and/or administration personnel who maintain logical access functions.
- 1I. PIH should ensure the PIC security module and the SQL Server 2000 incorporate the following identification and authentication controls:
  - Password length is set to a minimum of eight characters.
  - Passwords are set to expire every 60 days or less.
  - Passwords are required to contain special characters, not be in an online dictionary, and unrelated to the user ID.
  - Passwords are made inactive after three unsuccessful login attempts.

- A history file functionality is established to ensure that previously used passwords are not used again.
- User accounts or IDs that have been inactive over a period of six months are disabled. User accounts that are inactive over a period of 12 months should be permanently disabled.
- All users are given individual and distinct user IDs to ensure user accountability.

We recommend that the Assistant Secretary of Public and Indian Housing, in coordination with the Office of Chief Information Officer:

- 1J. Ensure adequate separation of duties by separating the processes for account setup and authorization so that PIH does not control both functions.
- 1K. Ensure that the access controls over the SQL Server 2000 are strengthened by using the audit log function capability under the current release version of the SQL Server 2000, to include enabling of the C2 auditing mode feature.
- 1L. Develop an alternative to SQL Server 2000 security mode, which has weak authentication controls. An alternative would be to use "Mixed Mode". Mixed Mode combines the SQL Server 2000 and Windows 2000 IDs using robust access controls of Windows 2000.

# Auditee Comments

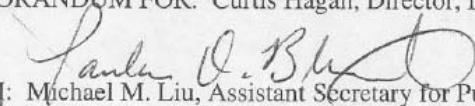


U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT  
WASHINGTON, DC 20410-5000

AUG - 5 2003

ASSISTANT SECRETARY FOR  
PUBLIC AND INDIAN HOUSING

MEMORANDUM FOR: Curtis Hagan, Director, Information System Audit Division, GAA

FROM:   
Michael M. Liu, Assistant Secretary for Public and Indian Housing, P

SUBJECT: Draft Audit Report on HUD's Public and Indian Housing Information Center (PIC)  
Security Maintenance Sub-Module

This memorandum is a response to your draft audit report for the recently completed audit of controls over the security of HUD's Public and Indian Housing Information (PIH) Center (PIC). The attached documents combine the recommendations organic to the draft audit report and comments from PIH and the Chief Information Officer Office as requested.

If you have any questions, please contact David Moore at 708-0614, extension 4158.

Attachments

cc: Vickers B. Meadows, Assistant Secretary for Administration, A

## Response to IG Report on PIC System

Thank you for the opportunity to review your draft audit on the Public and Indian Housing Information Center (PIC) focusing on the security of the system. The Office of Public and Indian Housing (PIH) agrees that it needs to take steps to enhance the security in the PIC system further.

As you know, the PIC system has a security architecture which is comparable with other HUD web applications and employs standard industry based internet security features including: login identification and password that grants users access to the system; 128 bit Secure Socket Layer encryption of the transmission of the login identification and password; restricted access to the system based on user roles; 128 bit Secure Socket Layer encryption of the transmission of privacy act sensitive data on resident demographics; as well as firewall protection of the hardware infrastructure supporting the application. In addition it should be noted that staff reporting to the Office of the Chief Information Officer (OCIO) routinely applies necessary upgrades and patches to protect the infrastructure supporting PIC as well as performs independent intrusion tests.

There is, as the report notes, a need for improvement in PIC security given that it is a repository of data subject to the requirements of the Privacy Act and that the threat in relation to Cyber-Security has increased in light of the events of September 11, 2001 and the war on terror. PIH also acknowledges that it did not go through a documented, rigorous analysis of the security required prior to developing the PIC system but rather went through an informal process that adopted existing security models with inadequate analysis of the potential risk. PIH therefore agrees with most of the recommendations included in the draft report. Where PIH disagrees, the disagreements primarily relate to the specific parameters proposed in a given recommendation rather than the need to have parameters.

PIH's response to the specific recommendations is as follows:

### Recommendations:

- 1A. Conduct a comprehensive security review of the PIC system. This review should include conducting sensitivity and risk assessments and formulating comprehensive security policy and goals. This security review should be used to form the basis for developing comprehensive security policies and procedures, security standards, and controls to ensure that PIC system critical data and resources are adequately safeguarded against waste, fraud, or abuse.**

### Response:

PIH agrees with the recommendation and has already initiated plans for a risk assessment of PIC and a NIST compliant 800-18 Security Plan with attendant policies and procedures.

- 1B. Conduct a review of the roles and responsibilities and access rights based on the business rules and the sensitivity of the data. From this review, build SQL queries based on the security logic design to establish a process to monitor user's access.**

**Response:**

PIH agrees with the recommendation.

- 1C. Remove the application Security Administration function from the PHAs and the vendors and assign it to HUD personnel only.**

**Response:**

PIH agrees with the recommendation; however, it should be noted that this is a significant change that will require extensive coordination with the Office of the Chief Information Officer and the allocation of adequate staffing for the increased workload associated with the transfer of this function.

- 1D. Establish a comprehensive process for monitoring and validating, on a semi-annual basis, users access to the PIC system. This re-certification process should include developing policies and procedures that include (a) developing access control lists of users (including groups, machines, processes), (b) how access to the system should be requested, granted and what information should be obtained and maintained on users, (c) limiting access granted to users outside the HUD organization to predefined roles with access levels determined and approved by HUD staff, and (d) specifics regarding who can be assigned security administration rights within the system and how this access will be monitored.**

**Response:**

PIH generally agrees with the recommendation; however, it intends to explore an alternative approach with respect to the time period for monitoring and validating user access. PIH proposes to implement a tiered recertification approach. The vast majority of PIC users fall into the category of frequent users requiring semi-annual validations with the requirement of recertification as necessary. However, PIC has some critical infrequent users (i.e. PHA executive directors) who use PIC on a less frequent basis in line with the annual fiscal year cycle of PHAs. PIH intends to explore with the Inspector General's office the possibility of extending the time period beyond the semi-annual timeframe recommended but with alternate security controls.

- 1E. Ensure controls are in place for the creation and assignment of roles in the Security Administration sub-module. Additionally, roles in the Security Administration sub-module that are not utilized or are duplicative should be removed. Also, roles should be fully described to determine what they were created for.**

**Response:**

PIH agrees with the recommendation.

- 1F. Perform a review of the roles and responsibilities of PIC users and establish policies and procedures that identifies and defines global roles within the PIC system that maintain a proper segregation of duties to include (a) ensuring HUD security administrators do not have the ability to submit Form HUD-50058 data, and (b) creating separate global System and Security Administration roles within the PIC organization that divides responsibility for data correction and system security functions.**

**Response:**

PIH agrees with the recommendation with a limited exception. PIH needs to continue a business practice of supporting primarily small Public Housing Authorities with the submission of their 50058 data in limited situations. PIH intends to explore with the Inspector General instituting appropriate controls in such limited instances to address the separation of duties concern raised. PIH has already separated security administrator as opposed to system administrator roles and data correction procedures.

- 1G. Establish system specific policies and procedures for maintaining and controlling the confidentiality of user passwords and IDs.**

**Response:**

PIH agrees with the recommendation.

- 1H. Establish policies, procedures and standards for reviewing audit logs and that audit logs should be reviewed by personnel other than security and /or administration personnel who maintain logical access functions.**

**Response:**

PIH agrees with the recommendation.

- II. PIH should ensure the PIC security module and the SQL Server 2000 incorporates the following identification and authentication controls:**
- Password length is set to a minimum of eight characters.
  - Passwords are set to expire every 21 days.
  - Passwords are required to contain special characters, not be in an online dictionary, and unrelated to the user ID
  - Passwords are made inactive after three unsuccessful login attempts
  - A history file functionality is established to ensure that names, words, or old passwords (24 generations) are not reused.
  - Inactive user IDs for after six months are permanently disabled.
  - All users are given individual distinct IDs to ensure user accountability.

**Response:**

PIH agrees with the recommendation to strengthen identification and authentication controls; however it believes that the specific parameters recommended may not be appropriate in some instances given the nature of the application as a web enabled application rather than a local area network application. Many PIC users can only be expected to interact with PIC on a monthly or quarterly basis. PIH believes that a number of the parameters recommended may be too stringent for such users. It intends to explore with the Inspector General and HUD's OCIO security office implementing somewhat less stringent parameters that are more appropriate in relation to more infrequent users. The specific parameters that are in question are underlined in the following list: the requirement for passwords to expire every 21 days; the requirement that passwords be made inactive after three unsuccessful login attempts; the requirement that 24 generations of passwords not be reused; the recommendation that user identifications be permanently disabled after six months of inactivity. PIH also notes that although it agrees with the recommendation that all users are to be given individual distinct user identifications, that it may face practical difficulty in carrying that recommendation out without being able to collect the social security numbers of PIC users. PIH believes based on a recent opinion circulated by HUD's Office of General Counsel that it is precluded from collecting social security numbers from non-HUD users of PIC.

- 1J. Ensure adequate separation of duties by separating the processes for account setup and authorization so that PIH does not control both functions.**

**Response:**

PIH and the OCIO agree with the recommendation. Discussions have already started with the HUD-OCIO security office to establish this process.

- 1K. Ensure that the access controls over the SQL Server 2000 are strengthened by using the audit log function capability under the current release version of the SQL Server 2000, to include enabling of the C2 auditing mode feature.**

**Response:**

PIH and HUD's OCIO agree to investigate and implement additional auditing features in the SQL Server 2000 database subject to system technical and performance feasibility.

- 1L. Develop an alternative to SQL Server 2000 security mode, which has weak authentication controls. An alternative would be to use "Mixed Mode". Mixed Mode combines the SQL Server 2000 and Windows 2000 IDs using robust access controls of Windows 2000.**

**Response:**

PIH and HUD's OCIO agree with the recommendation.

# Description of Microsoft SQL Server 2000 C2 Evaluation

For background information on the Microsoft SQL Server 2000 C2 Evaluation (the associated criteria of which is used for the auditing setting within the application), please refer to Microsoft's detailed description shown below:

## Microsoft SQL Server 2000 C2 Evaluation

In August, 2000, the US Government announced that Microsoft SQL Server 2000 had completed a successful evaluation at the C2 level according to the Trusted Database Interpretation (TDI) of the Trusted Computer System Evaluation Criteria (TCSEC).

The C2 evaluation applies to the originally-released version of SQL Server 2000 - that is, no service packs or patches need to be installed - when configured per the [Trusted Facility Manual](#) and running on Windows NT 4.0 in any of its [C2-evaluated configurations](#).

The TCSEC provides an evaluation by an independent third party against standardized criteria and according to a formal methodology known as the Trust Technology Assessment Program (TTAP). The evaluation carries the imprimatur of a trusted third party that has scrutinized the product and assessed the security it can provide. Microsoft worked with SAIC, an approved TTAP laboratory, to ensure that it fully met all documentation and testing requirements.

The TTAP evaluates the security features that a product provides and the assurance that the product correctly and fully implements them. The security features that are required at the C2 level include:

- Mandatory identification and authentication of all users on the system - The ability of the system to identify authorized users and to allow only them to access system resources
- Discretionary access control - The ability for users to protect their data as they desire.
- Accountability and Auditing - The ability of the system to thoroughly audit user and system actions.
- Object Reuse - The ability of the system to prevent users from obtaining information from resources that previously were used by others, for example, memory that has been released or files that have been deleted.

The assurance requirements at the C2 level include:

- Examination of source code
- Examination of detailed design documentation
- Retesting to ensure that any errors identified during the evaluation have been corrected.
- Penetration testing

The following information regarding the C2 evaluation for SQL Server 2000 is available for review:

- [TCSEC Evaluation Summary](#)
- [Final Evaluation Report](#)
- [Trusted Facility Manual](#) for SQL Server 2000 C2 Evaluation.

For more information on the TCSEC process, see <http://www.radium.ncsc.mil/tpep/>.

Source: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/db/sql/sqlc2.asp>