

**GAO**

Report to the Acting Director of the  
Federal Housing Finance Agency

---

April 2010

# INFORMATION SECURITY

Opportunities Exist  
for the Federal  
Housing Finance  
Agency to Improve  
Controls



**GAO**

Accountability \* Integrity \* Reliability

---



Highlights of [GAO-10-528](#), a report to the Acting Director of the Federal Housing Finance Agency

## Why GAO Did This Study

The Federal Housing Finance Agency (FHFA) relies extensively on computerized systems to carry out its mission to provide effective supervision, regulation, and housing mission oversight of the Federal National Mortgage Association (Fannie Mae), the Federal Home Loan Mortgage Corporation (Freddie Mac), and the federal home loan banks. Effective information security controls are essential to ensure that FHFA's financial information is protected from inadvertent or deliberate misuse, disclosure, or destruction.

As part of its audit of FHFA's fiscal year 2009 financial statements, GAO assessed the effectiveness of the agency's information security controls to ensure the confidentiality, integrity, and availability of the agency's financial information. To do this, GAO examined FHFA information security policies, procedures, and other documents; tested controls over key financial applications; and interviewed key agency officials.

## What GAO Recommends

GAO recommends that the Acting Director of the FHFA take steps to mitigate control deficiencies and fully implement a comprehensive information security program.

In commenting on a draft of this report, FHFA agreed with GAO's findings and stated that it plans to address the identified deficiencies.

[View GAO-10-528 or key components.](#)  
For more information, contact Gregory C. Wilshusen at (202) 512-6244 or [wilshuseng@gao.gov](mailto:wilshuseng@gao.gov), or Dr. Nabajyoti Barkakati at (202) 512-4499 or [barkakatin@gao.gov](mailto:barkakatin@gao.gov).

## INFORMATION SECURITY

### Opportunities Exist for the Federal Housing Finance Agency to Improve Controls

#### What GAO Found

Although FHFA has implemented important information security controls, it has not always implemented appropriate controls to sufficiently protect the confidentiality, integrity, and availability of financial information stored on and transmitted over its key financial systems, databases, and computer networks. The agency's financial system computing environment had deficiencies in several areas and the controls that were in place were not always effectively implemented to prevent, limit, and detect unauthorized access to the agency network and systems. Specifically, FHFA did not always maintain authorization records for network and system access, enforce the most restrictive access needed by users on shared network files and directories, and enforce the most restrictive set of rights needed by users to perform their assigned duties. Further, it did not effectively implement physical protection and environmental safety controls over its facilities and information technology resources. GAO identified numerous instances in which FHFA facilities were not adequately secured and was able to obtain unauthorized access from outside agency facilities into the agency's interior space containing sensitive information and information technology equipment. FHFA officials acknowledged these shortcomings and indicated that the agency has taken steps or is planning to take steps to mitigate these deficiencies.

A key reason for the control deficiencies in FHFA's financial system computing environment is that the agency has not yet fully implemented its agencywide information security program to ensure that controls are appropriately designed and operating effectively. Although FHFA made important progress in developing and documenting elements of its information security program, written policies, procedures, and technical standards do not reflect the current operating environment. Further, the agency has not yet developed, documented, and implemented sufficient policies and procedures to ensure that the activities performed by external third parties are monitored for compliance with FHFA's policies. Although these deficiencies were not considered significant deficiencies for financial reporting purposes, if left uncorrected they unnecessarily increase the risk that sensitive and financial information is subject to unauthorized disclosure, modification, or destruction.

---

# Contents

---

<b>Letter</b>		<b>1</b>
	Background	2
	Opportunities for Improvement in Information Security Controls	5
	Conclusions	19
	Recommendations for Executive Action	19
	Agency Comments	21
<b>Appendix I</b>	<b>Objective, Scope, and Methodology</b>	<b>23</b>
<b>Appendix II</b>	<b>Comments from the Federal Housing Finance Agency</b>	<b>25</b>
<b>Appendix III</b>	<b>GAO Contacts and Staff Acknowledgments</b>	<b>26</b>

---

## Abbreviations

BPD	Bureau of the Public Debt
Fannie Mae	Federal National Mortgage Association
FHFA	Federal Housing Finance Agency
FHFB	Federal Housing Finance Board
FISMA	Federal Information Security Management Act of 2002
FMS	financial management system
Freddie Mac	Federal Home Loan Mortgage Corporation
HUD	Department of Housing and Urban Development
IT	information technology
NIST	National Institute of Standards and Technology
OFHEO	Office of Federal Housing Enterprise Oversight

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office  
Washington, DC 20548

April 30, 2010

Mr. Edward J. DeMarco  
Acting Director  
Federal Housing Finance Agency

Dear Acting Director DeMarco:

The Housing and Economic Recovery Act of 2008<sup>1</sup> established the Federal Housing Finance Agency (FHFA) on July 30, 2008, and charged it with the supervisory and regulatory oversight of Federal National Mortgage Association (Fannie Mae), Federal Home Loan Mortgage Corporation (Freddie Mac), and the 12 federal home loan banks. The act requires the agency to annually prepare and submit financial statements to the Director of the Office of Management and Budget, and requires us to audit the agency's financial statements.

As part of our audit of FHFA's fiscal year 2009 financial statements,<sup>2</sup> we assessed the effectiveness of the agency's information security controls<sup>3</sup> over its financial information. In our report on the agency's financial statements for fiscal year 2009, we concluded that FHFA had effective internal control over financial reporting as of September 30, 2009. We also determined that the agency's system of internal control had certain deficiencies, although we did not consider those to be material

---

<sup>1</sup>Pub. L. No. 110-289, 122 Stat. 2654 (July 30, 2008).

<sup>2</sup>GAO, *Financial Audit: Federal Housing Finance Agency's Fiscal Year 2009 Financial Statements*, [GAO-10-218](#) (Washington, D.C.: Nov. 16, 2009).

<sup>3</sup>Information security controls include logical and physical access controls, configuration management, segregation of duties, and continuity of operations. These controls are designed to ensure that access to information is appropriately restricted, that physical access to sensitive computing resources and facilities is protected, that only authorized changes to computer programs are made, that incompatible duties are segregated among individuals, and that backup and recovery plans are adequate to ensure the continuity of essential operations.

---

weaknesses or significant deficiencies<sup>4</sup> for financial reporting purposes. These deficiencies included matters related to access controls and information security management.

In this report, we provide additional details on FHFA's information security controls, including details on information security deficiencies in the agency's system of internal control over financial reporting. Our specific objective was to assess the effectiveness of the agency's controls for ensuring the confidentiality, integrity, and availability of its financial information. We performed our work at agency facilities in Washington, D.C., and at financial application servicing and commercial hosting facilities in Parkersburg, West Virginia, and Austin, Texas. Our work was conducted from February 2009 to April 2010 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. See appendix I for additional details on our objective, scope, and methodology.

---

## Background

Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. It is especially important for government agencies, where maintaining the public's trust is essential. The dramatic expansion in computer interconnectivity and the rapid increase in the use of the Internet have revolutionized the way our government, our nation, and much of the world communicates and conducts business. Although this expansion has created many benefits for agencies such as FHFA in achieving their missions and providing information to the public, it also exposes federal networks and systems to various threats.

---

<sup>4</sup>A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented or detected and corrected on a timely basis. A significant deficiency is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect and correct misstatements on a timely basis.

---

Without proper safeguards, computer systems are vulnerable to individuals and groups with malicious intent who can intrude and use their access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. The risks to these systems are well-founded for a number of reasons, including the dramatic increase in reports of security incidents, the ease of obtaining and using hacking tools, and steady advances in the sophistication and effectiveness of attack technology. The Federal Bureau of Investigation has identified multiple sources of threats, including foreign nation states engaged in intelligence gathering and information warfare, domestic criminals, hackers, virus writers, and disgruntled employees or contractors working within an organization. In addition, the U.S. Secret Service and the CERT<sup>®</sup> Coordination Center<sup>5</sup> studied insider threats in the government sector and stated in a January 2008 report that “government sector insiders have the potential to pose a substantial threat by virtue of their knowledge of, and access to, employer systems and/or databases.”

Our previous reports, and those by federal Inspectors General, describe persistent information security weaknesses that place federal agencies at risk of disruption, fraud, or inappropriate disclosure of sensitive information. Accordingly, we have designated information security as a governmentwide high-risk area since 1997, most recently in 2009.<sup>6</sup>

Recognizing the importance of securing federal agencies’ information systems, Congress enacted the Federal Information Security Management Act (FISMA) in December 2002<sup>7</sup> to strengthen the security of information and systems within federal agencies. FISMA requires each agency to develop, document, and implement an agencywide information security program for the information and information systems that support the operations and assets of the agency, using a risk-based approach to information security management. Such a program includes assessing risk; developing and implementing cost-effective security plans, policies, and

---

<sup>5</sup>The CERT<sup>®</sup> Coordination Center is a center of Internet security expertise located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

<sup>6</sup>GAO, *High-Risk Series: Information Management and Technology*, [GAO/HR-97-9](#) (Washington, D.C.: February 1997) and GAO, *High Risk Series: An Update*, [GAO-09-271](#) (Washington, D.C.: January 2009).

<sup>7</sup>FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No. 107-347, Dec. 17, 2002.

---

procedures; providing specialized training; testing and evaluating the effectiveness of controls; planning, implementing, evaluating, and documenting remedial actions to address information security deficiencies; and ensuring continuity of operations.

---

## FHFA Relies on Information Technology to Fulfill Its Mission

The Housing and Economic Recovery Act of 2008 created the FHFA, an independent federal regulatory agency resulting from the statutory merger of the Federal Housing Finance Board (FHFB) and the Office of Federal Housing Enterprise Oversight (OFHEO). FHFA absorbed the powers and regulatory authority of both entities, with expanded legal and regulatory authority. The act also gave FHFA the responsibility for, among other things, the supervision and oversight of Fannie Mae, Freddie Mac, and the 12 federal home loan banks. Specifically, the agency was assigned responsibility for ensuring that each of the regulated entities operates in a fiscally safe and sound manner, including maintenance of adequate capital and internal controls, and carries out its housing and community development finance mission.

FHFA is a small government agency with a workforce that includes economists, market analysts, examiners, subject matter experts, technology specialists, accountants, and attorneys. FHFA had a staff of about 430 employees at the end of fiscal year 2009.

During fiscal year 2009, OFHEO's and FHFB's personnel, property, and program activities, and certain employees and activities of the Department of Housing and Urban Development (HUD), were transferred to FHFA. The assets, liabilities, and financial transactions of OFHEO and FHFB were also consolidated into FHFA. To support these activities, FHFA began unifying the agency's information technology (IT) infrastructure operations, including integrating its general support systems, and has made substantial progress. This effort included implementing an integrated e-mail messaging system, consolidating software licenses and services, eliminating duplication of information systems and sources, and unifying internal customer service operations.

FHFA also unified its financial systems. FHFA uses the National Finance Center, a service provider within the Department of Agriculture, for its payroll and personnel processing. During fiscal year 2009, the agency coordinated programming and systems changes with the National Finance Center to achieve a transition from two separate systems into a unified payroll and processing system for the agency with integration completed in July 2009.

---

FHFA had been using legacy financial management systems and processes from OFHEO and FHFBS. In fiscal year 2009, FHFA completed outsourcing of its financial management services to the Treasury Department's Bureau of the Public Debt (BPD) Administrative Resource Center and a new financial management system (FMS),<sup>8</sup> which became operational in July 2009. FMS provides the agency with an integrated system for its accounting, procurement, and travel activities. The system uses Oracle Corporation's hosting service in Austin, Texas. As the commercial hosting facility for the Administrative Resource Center's financial management services, Oracle staff serve as database and systems administrators and provide backup and recovery services for FHFA's financial information.

---

## Opportunities for Improvement in Information Security Controls

A basic management objective for any organization is to protect the resources that support its critical operations from unauthorized access. Organizations accomplish this objective by designing and implementing controls that are intended to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities. Such controls include both logical access and physical access controls. Logical access controls include requiring users to authenticate themselves and limiting the files and other resources that authenticated users can access and the actions that these users can execute. Physical access controls involve restricting physical access to computer resources and protecting these resources from intentional or unintentional loss or impairment. Without adequate access controls, unauthorized individuals, including external intruders and former employees, can surreptitiously read and copy sensitive information and make undetected changes or deletions for malicious purposes or personal gain. In addition, authorized users can intentionally or unintentionally read, add, delete, modify, or execute changes that are outside their span of authority.

FHFA has multiple deficiencies in the access controls intended to restrict logical and physical access to the agency's information and systems. A major reason for these control deficiencies was that FHFA did not fully implement key activities of its information security program. If left uncorrected, the deficiencies increase the risk that unauthorized

---

<sup>8</sup>FMS is based on BPD's financial management services which use the Oracle E-Business Suite. In addition to security controls provided by FMS and common controls provided by its general support system, FMS security relies on security controls developed and maintained by BPD for the Oracle E-Business Suite and security controls developed and maintained by Oracle Corporation for its commercial hosting services.



---

individuals may gain access to FHFA computing resources, programs, information, and facilities.

---

## Deficiencies in Controlling Logical Access May Put Information Resources at Risk

Authorization is the process of granting or denying access rights and permissions to a protected resource, such as a network, a system, an application, a function, or a file. A key component of granting or denying access rights is the concept of “least privilege” which is a basic principle for securing computer resources and information. This principle means that users are granted only those access rights and permissions they need to perform their official duties. To restrict legitimate users’ access to only those programs and files they need to do their work, organizations establish access rights and permissions. “User rights” are allowable actions that can be assigned to users or to groups of users. File and directory permissions are rules that regulate which users can access a particular file or directory and the extent of that access. To avoid unintentionally authorizing users’ access to sensitive files and directories, an organization must give careful consideration to its assignment of rights and permissions. Furthermore, National Institute of Standards and Technology (NIST) Special Publication 800-53<sup>9</sup> states that system access should be granted based on a valid access authorization and intended system usage and the most restrictive access needed by users for accounts, files, and directories needs to be enforced. Finally, FHFA policy requires that information systems enforce the most restrictive set of rights needed by users to perform their assigned duties.

FHFA implemented numerous controls to prevent, limit, and detect logical access to its financial systems and information. For example, it enforced the use of (1) network user names and complex passwords, and (2) two-factor authentication<sup>10</sup> for remote access to FHFA’s networks. In addition, wireless access to the network is prohibited inside the FHFA facilities unless approved by the Chief Information Officer or the Chief Information Security Officer.

---

<sup>9</sup>NIST, *Recommended Security Controls for Federal Information Systems and Organizations*, SP 800-53 Rev. 3 (Gaithersburg, Md., August 2009).

<sup>10</sup>Two-factor authentication is a way of verifying someone’s identity by using two of the following: something the user knows (password), something the user has (badge), or something unique to the user (fingerprint).

---

However, deficiencies in controlling logical access diminished the effectiveness of these controls and placed information resources at risk. For example, FHFA did not always maintain authorization records for network and system access, enforce the most restrictive access needed by users on shared network files and directories, and restrict access to sensitive system resources. To illustrate:

- FHFA did not maintain network access authorizations for every agency network user and authorization records contained notes that indicated records were incomplete. Specifically, the agency could not provide authorization for 20 of 30 users reviewed. If network and system access authorizations are not fully documented and monitored, increased risk exists that users may be granted unauthorized and unintended network and system access.
- FHFA established server files and directories that allowed network users to access agency and regulated-entity confidential information even though such users did not have a business need for this information. To illustrate, using network accounts with access privileges normally granted to all network end users, we were able to access sensitive and confidential regulatory information—including internal meeting notes, a mortgage market analysis, and a liquidity report for a regulated entity—on a server which hosted a FHFA examiner support system. Additionally, we were able to read documents labeled confidential on a shared drive. The network accounts were also unnecessarily given the rights to access and modify database files on a system the agency uses for financial analysis. By not restricting access to this confidential information to only personnel with an authorized need for access, FHFA risks the possibility that sensitive information could be used for unintended purposes, which could impact the ability of the agency to carry out its organizational mission.
- FHFA did not always sufficiently restrict system rights to only those needed by users to perform their assigned duties. For example, the agency did not sufficiently restrict user access to privileged accounts. Local user network accounts had rights that permitted the user to create new local workstation accounts and then escalate these accounts to have local administrator privileges. These accounts could then be used to create privileged accounts on other agency workstations by remotely connecting to them. This would allow malicious insiders to grant themselves or others access to sensitive information technology and communications resources. Local administrator accounts could also be used to install unauthorized software that could disrupt agency operations and capture various user credentials, such as those used to access the agency's financial applications. The Chief Information Officer's office stated that

---

this deficiency existed because users were given privileged access to their workstations to facilitate the agency's integration of its general support systems. It also stated the privileged access was only intended for temporary use and the fact that the access was not removed after the integration phase was completed was an error.

FHFA informed us it is currently developing an access control procedure to revalidate user access levels for network and system access. FHFA plans to finalize this procedure as part of future phases of integrating its general support systems. According to agency officials, this should occur by June 2010. Officials also said that access has been restricted to (1) administrators, (2) application users, or (3) specific agency personnel based on input from information owners. However, until these control procedures are fully developed, effectively implemented, and continuously monitored, FHFA will remain at increased risk of individuals gaining unauthorized access to information resources.

---

### Deficiencies in Physical Security and Environmental Safety Controls Reduced Control Effectiveness

Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. These controls involve restricting physical access to computer resources and sensitive information, usually by limiting access to the buildings and rooms in which the resources are housed and periodically reviewing access rights granted to ensure that access continues to be appropriate based on established criteria. NIST policy requires that federal organizations implement physical security and environmental safety controls to protect employees and contractors, information systems, and the facilities in which they are located. FHFA policy also requires access controls for deterring, detecting, monitoring, restricting, and regulating access to areas housing sensitive IT equipment and information.

FHFA effectively secured some of its sensitive areas and computer equipment and took other steps to provide physical security and environmental safety. For example, FHFA issued electronic badges to help control access to many of its sensitive and restricted areas. The agency also drafted procedures to guide staff in securing their office space and protecting sensitive information. In addition, the agency implemented environmental and safety controls such as temperature and humidity controls, as well as emergency lighting to protect its staff and sensitive IT resources.

---

---

FHFA Did Not Sufficiently Secure Areas Containing IT Equipment and Sensitive Information

However, FHFA did not effectively (1) secure areas with IT equipment, (2) complete physical security and environmental control policies, (3) perform physical security risk assessments, (4) authorize and control physical access to resources and information, (5) detect potential security incidents, (6) implement a visitor control program, (7) enforce physical security safeguards, (8) secure locations that support computer operations, or (9) implement fire protection controls.

Sensitive areas at FHFA were not sufficiently secured. NIST Special Publication 800-53 requires that federal organizations control physical access points, including designated entry and exit points, to the facility where information systems reside. NIST also requires that organizations enforce stringent physical access measures for areas within a facility containing large concentrations of information system components, such as server rooms and communications centers. NIST further requires that organizations position information system components in locations within its facilities to minimize the opportunity for unauthorized access. In addition, FHFA policy requires that access to its facilities housing sensitive IT equipment and information be limited to authorized personnel and that its employees take steps to prevent unauthorized access or disclosure of information.

However, numerous instances existed in which FHFA did not sufficiently secure its facilities. During our testing, we were able to obtain unauthorized access from outside FHFA facilities into its interior space containing sensitive information and IT equipment.

- *Entrance security.* Security for building entrances was not sufficient. We were able to obtain unauthorized access to FHFA's facilities on three different dates when we performed unescorted visits. Guards were either not on duty or did not inspect credentials and verify identities at each of the agency's three downtown Washington, D.C., buildings. Two locations had concierge staff in their lobbies during regular business hours, but they did not require or check credentials. Agency staff were not present at these locations during early morning visits on two separate dates. A security officer was present during one visit and permitted us access with an expired badge. Guards on duty at one location did not require that we display identification during multiple visits to the facility. Further, no magnetometers or X-ray machines were available, nor did we observe visitors being searched at any location, creating the potential that an adversary could bring dangerous materials (e.g., firearms, explosives, or chemical and biological agents) into these facilities without being detected, challenged, or hindered from entering.

- 
- *Interior security.* Office space at each of the three FHFA Washington, D.C., buildings containing sensitive documents and IT equipment was either unsecured or had very weak security features. We obtained entry to FHFA interior space by pushing on interior doors, using commonly available items to defeat security mechanisms, or walking behind employees. On one visit to office space at an agency location, we walked past inattentive guards who did not challenge us and walked through unsecured interior doors to obtain access. Inside the secured space, many agency staff left their offices unsecured, including some who left sensitive information on their desks.
  - *Computer room security.* FHFA space containing sensitive computer equipment was not appropriately secured. We were able to obtain entry to an agency server room and storage area on three separate occasions by using commonly available items. This security deficiency was further compounded because the agency located the server room near an elevator area such that the public could easily obtain access to the general area where the server room is located.

Because areas containing sensitive IT equipment and information were not appropriately secured, FHFA has less assurance that computing resources are protected from inadvertent or deliberate misuse including fraud or destruction.

#### FHFA Physical Security and Environmental Control Policies Were Incomplete

NIST Special Publication 800-53 requires that organizations develop formal documented physical security policies and procedures to facilitate the implementation of physical and environmental protection controls. NIST also requires that these policies be consistent with all applicable mandates and regulations.

However, FHFA's physical security and environmental control policies for the protection of its assets—including sensitive computer equipment, as well as employees, contractors, visitors, and the general public—were incomplete. FHFA policies did not adequately describe requirements for physically protecting IT equipment in sensitive locations. For example, FHFA policies did not

- describe how to respond to a physical security intrusion or report suspected or confirmed breaches in physical security;
- require that computer room authorization lists be periodically reviewed to determine if staff previously authorized access still require access or should be removed from the lists; and

- 
- provide clear and consistent guidance for developing and implementing environmental safety controls, such as fire protection and emergency power and lighting for its facilities housing computer rooms.

Until such policies are approved and implemented, FHFA has less assurance that its staff has sufficient and appropriate guidance to effectively and consistently protect its computing resources from inadvertent or deliberate misuse, including fraud or destruction.

#### FHFA Did Not Perform Physical Security Risk Assessments for Its Facilities

Identifying and assessing physical security risks are essential to determining what controls are required and what levels of resources should be expended on controls. NIST requires that organizations assess physical security risks to their facilities when they perform required risk assessments of their information systems. According to NIST Special Publication 800-30, the physical security environment of information systems should be considered when selecting cost-effective security controls.

However, FHFA did not perform physical security risk assessments for its three Washington, D.C., facilities that house computer rooms and sensitive information. Although FHFA officials stated that the landlords of their leased facilities performed risk assessments, they acknowledged that the assessments did not cover the space FHFA uses nor did FHFA obtain and review those assessments. Until risk assessments are performed and used to help determine what physical security controls should be implemented, FHFA has less assurance that computing and other resources are consistently and effectively protected from inadvertent or deliberate misuse.

#### Physical Access to Sensitive Computer Resources and Information Was Not Effectively Authorized and Controlled

NIST requires that organizations control all physical access points to its computer facilities and verify individual access authorizations. However, at one of its locations, FHFA did not fully control physical access authorizations to facilities containing sensitive computer resources and information and did not maintain a current list of personnel with authorized access to its facilities' server rooms. Further, FHFA did not periodically review the authorization lists to determine if staff who were previously authorized access to the server rooms still required access or could be removed from the list.

---

Several instances occurred where individuals inappropriately entered sensitive areas. For example:

- Seven individuals accessed four rooms containing IT equipment without authorization;
- Seven access cards with generic names were used to access two rooms containing sensitive IT equipment. FHFA was unable to identify who actually used the cards and accessed the rooms;
- Someone used a terminated employee's access card seven times to access two rooms containing sensitive IT equipment. FHFA was unable to determine who used the card and accessed the rooms; and
- FHFA's landlord for one facility had the ability to grant physical access to sensitive IT areas, and granted non-FHFA individuals access to the IT workroom without the agency's knowledge. Physical access logs showed that five of the landlord's staff were not on FHFA's authorization list, but had entered the workroom without agency knowledge.

As a result of these collective deficiencies, sensitive areas were accessed by unauthorized individuals and are at increased risk of further unauthorized access that could result in critical computing resources and sensitive information being inadvertently or deliberately misused or destroyed.

FHFA Was Unable to Sufficiently Detect and Respond to Potential Physical Security Incidents

NIST Special Publication 800-53 requires that organizations monitor physical access to their information systems to detect and respond to physical security incidents. For higher risk areas such as computer rooms, NIST requires organizations to monitor real-time intrusion alarms and surveillance equipment and/or employ automated mechanisms to recognize potential intrusions. FHFA policy also requires that controls be implemented to detect and monitor access to areas housing sensitive IT equipment and information.

However, FHFA did not have processes and procedures, or in some instances, surveillance equipment, to monitor physical access to its Washington, D.C., computer rooms and areas containing sensitive documents so that it could detect and respond to physical security incidents. FHFA did not have monitoring or surveillance equipment, such as a closed circuit television at entrance doors, nor were the doors centrally or locally alarmed at two of the locations. Additionally, agency staff members were not reviewing access logs to sensitive IT areas, as

---

required by NIST, and there was no procedure in place to guide such reviews. If agency staff had reviewed access logs, they may have been able to ascertain that unauthorized individuals were actually accessing agency computer rooms as discussed above. Further, the monitoring system that FHFA was using did not have the ability to generate physical access logs for the primary server room at one location. As a result, increased risk exists that unauthorized access and physical security incidents would not be detected or effectively investigated.

**FHFA Did Not Effectively Control Visitors at One Facility**

NIST Special Publication 800-53 requires that organizations properly authenticate visitors before they can access facilities containing sensitive information systems. FHFA policy also requires that all visitors be escorted and sign in and out while visiting FHFA facilities, with these records being maintained for at least one year. As required by NIST, these records should include the name, signature, and organization of the visitor; form(s) of identification; date of access; times of entry and departure; purpose of the visit; and name/organization of the person visited.

However, FHFA had no visitor control practices in place at one of its facilities. During three unaccompanied visits to this location we obtained access to and roamed freely throughout FHFA space without any identification or escort, and were not challenged by any staff. Further, FHFA did not require visitors to sign in or out, nor did it maintain visitor access records to its computer room or office space at one facility and its computer room at another facility. As a result, the agency was at increased risk of unauthorized visitors gaining access to sensitive areas and inadvertently or deliberately misusing or destroying critical computing resources.

**FHFA Employees Did Not Sufficiently Enforce Physical Security Safeguards**

NIST Special Publication 800-53 requires that organizations control physical access to areas containing sensitive information and system devices. NIST also requires that organizations verify individual access authorizations before granting access to its facilities.

However, FHFA employees did not always enforce physical security safeguards. For example, agency employees did not always use their badges to obtain access to electronically secured interior spaces. We observed agency staff who piggybacked into secured spaces when another individual held the door open for them on multiple occasions during three separate visits to FHFA locations. We also piggybacked into secured FHFA interior spaces behind other agency staff numerous times without any visible agency or visitor credentials. At no time were we challenged by FHFA staff and, in several cases, agency staff held doors open for us to



---

allow our entry without authenticating our identity and authority. In addition, on three separate visits to one agency location, we easily opened entry doors by applying slight force and a local alarm sounded. However, agency employees who were in the area either did not notice or disregarded the alarm when we entered the area. Because its employees did not sufficiently enforce effective physical security, FHFA has less assurance that computing resources and sensitive information are protected from inadvertent or deliberate misuse.

**Telecommunications and Electrical Closets that Support Computer Operations Were Not Sufficiently Secured**

NIST Special Publication 800-53 requires that organizations control access to information systems distribution and transmission lines within organizational facilities and protect power equipment and power cabling for information systems from damage and destruction.

However, FHFA did not secure two closets at one of its facilities that contain telecommunications wiring that supports its computer operations. FHFA also did not secure an electrical closet that contains power equipment and cabling at the same location. The power equipment controlled electrical power to FHFA's server room and office space. The electrical closet also contained a large amount of miscellaneous construction materials. After we notified FHFA of this problem, agency personnel stated that they had secured the closets and agreed to remove the stored materials, but two subsequent reinspections showed that the electrical closet remained unsecured and cluttered with construction materials. Because these spaces were not sufficiently secured, FHFA has less assurance that computer operations are protected from inadvertent or deliberate misuse including fraud or destruction.

**Fire Protection Controls Were Not Effectively Implemented in a Server Room**

FHFA did not adequately establish and implement controls to protect a server room containing sensitive IT equipment from potential fire damage. NIST Special Publication 800-53 requires that organizations employ and maintain fire suppression and detection devices for information systems. Agency policy also requires the use of controls to safeguard assets against various hazards including fire. However, FHFA did not have adequate fire suppression for its server room at one facility. According to FHFA staff, a fire suppression system was installed but did not function for over a year prior to our visit because repairs to the server room were required before the system could be activated. Subsequent to our visit, FHFA activated the fire suppression system in August 2009. Prior to this activation, sensitive IT equipment was at risk of damage which threatened the availability of critical information resources and information.

---

To their credit, senior FHFA officials acknowledged these physical security and environmental safety control shortcomings and told us that they have taken steps or are planning to take steps to mitigate most of the deficiencies. However, until they fully implement physical security controls, FHFA computer facilities and resources remain vulnerable to espionage, sabotage, damage, and theft.

---

### FHFA Has Not Fully Implemented All Elements of Its Information Security Program

A key reason for the information security deficiencies in FHFA's information systems discussed previously is that it has not yet fully implemented its agencywide information security program to ensure that controls are appropriately designed and operating effectively.

FISMA requires each agency to develop, document, and implement an information security program that, among other things, includes:

- policies and procedures that (1) are based on risk assessments, (2) cost effectively reduce information security risks to an acceptable level, (3) ensure that information security is addressed throughout the life cycle of each system, and (4) ensure compliance with applicable requirements; and
- plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

In addition, FISMA requires that the agency information security program encompass the information and information systems supporting the operations and assets of the agency that are provided or managed by another agency, contractor, or other source.

FHFA has made important progress in developing and documenting its policies and procedures for the agency's information security program. For example, it has published an Information Security Policy Handbook. The agency has begun putting procedures from the handbook in place and expects to fully implement these in fiscal year 2010. FHFA also developed and issued the agency's Breach Notification Policy and Plan for security incidents involving personally identifiable information. The agency also addressed security-related weaknesses for systems noted in the prior year OFHEO and FHFB FISMA reviews and completed a review to validate and document system configurations. FHFA also maintained current security

---

Policies, Procedures, Plans,  
and Technical Standards  
Related to Information Security  
do not Reflect the Current  
Operating Environment

---

certification and accreditations<sup>11</sup> on major financial systems that we reviewed. The certification and accreditation packages included evidence that FHFA tested management, operational, and technical controls and prepared security plans for its networks, facilities, and systems. According to FHFA, the agency also upgraded its Security Log Management System to monitor production servers and network device logs and security events. In addition, as part of a risk management approach to manage information technology assets, the agency implemented comprehensive scanning of production systems on a monthly basis to identify and correct system vulnerabilities. During the year, the agency expanded and improved its information security awareness training, providing a required automated training program to all employees and contractors.

However, policies, procedures, plans, and technical standards related to information security did not always reflect the current agency operating environment; and FHFA did not always effectively monitor its systems.

A key task in developing an effective information security program is to establish and implement policies, procedures, plans, and technical standards that govern security over an agency's computing environment. Developing, documenting, and implementing security policies are the primary mechanisms by which management communicates its views and requirements; these policies also serve as the basis for adopting specific procedures and technical controls. According to NIST Special Publication 800-53, these policies should include separation of incompatible duties, configuration management policies and procedures, and contingency plans.

Configuration management is an important control that involves the identification and management of security features for all hardware and software components of an information system at a given point and systematically controls changes to that configuration during the system's life cycle. Establishing controls over the modification of information system components and related documentation helps to prevent

---

<sup>11</sup>According to NIST, security certification and accreditation of information systems are important activities that support a risk management process and are an integral part of an agency's information security program. Security certification consists of conducting a security control assessment and developing the security documents. Security accreditation is the official management decision given by a senior agency official to authorize the operation of an information system and to explicitly accept the risk it may present to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls.

---

unauthorized changes and ensure that only authorized systems and related program modifications are implemented. This is accomplished by instituting policies, procedures, and techniques that help make sure all hardware, software, and firmware programs and program modifications are properly authorized, tested, and approved.

Contingency planning is another critical component of information protection. If normal operations are interrupted, network managers must be able to detect, mitigate, and recover from service disruptions while preserving access to vital information. A contingency plan is used to detail emergency response, backup operations, and disaster recovery for information systems. To be effective, these plans need to be clearly documented, communicated to potentially affected staff, and updated to reflect current operations. NIST also recommends continuity of operations and disaster recovery plans.

If properly implemented, policies and procedures should help reduce the risk that could come from unauthorized access or disruption of services. Technical security standards can provide consistent implementation guidance for each computing environment.

Although FHFA made important progress in developing and documenting elements of its information security program, its policies, procedures, plans, and technical standards related to separation of duties, configuration management, and continuity of operations do not reflect the current operating environment. For example:

- While FHFA had a separation of incompatible duties policy in place from the former FHFBS, the agency did not develop and document procedures for enforcing separation of duties. Agency officials stated that the agency has initiated a project to develop processes for the 18 security control families identified by NIST and will integrate separation of duties procedures into these processes; the expected completion date is June 2010.
- The agency did not finalize and approve configuration management policy and procedures. FHFA is using an interim change control and configuration process that was used at FHFBS and has developed a draft configuration management procedure; however, it has not been formalized and approved. Agency officials stated that a plan has been developed to train users and implement FHFA configuration management policy and procedures by May 2010.

- 
- Although FHFA has developed continuity of operations and disaster recovery plans, it has not formalized and approved them. Agency officials stated that a continuity of operations plan has been submitted to the senior agency leadership for review and comment and will be tested in May 2010. Based on the test results, it will be updated and finalized during the fourth quarter of fiscal year 2010. Also, a draft disaster recovery plan was approved in November 2009. The agency expects to test the plan in the summer of 2010.

In addition to actions mentioned above, agency officials indicate that FHFA will develop or update policies and procedures to reflect the current environment and to comply with NIST guidance by June 2010. Until the agency effectively develops, documents, and implements these policies, procedures, plans, and technical standards, it has less assurance that its systems and information are protected from unauthorized access or disruption of services.

#### FHFA Did Not Always Effectively Monitor Its Systems

FISMA states that each agency shall develop, document, and implement an agencywide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. The act specifically delineates federal agency responsibilities for (1) information collected or maintained by or on behalf of an agency and (2) information systems used or operated by an agency, by a contractor of an agency, or by another organization on behalf of an agency. Appropriate policies and procedures should be developed to ensure that the activities performed by external third parties are documented, agreed upon, implemented, and monitored for compliance.

FHFA did not perform effective oversight of the contractor's implementation of the security controls and program. Although FHFA developed a financial oversight document for FMS that outlined the assignment of activities between FHFA and the BPD, it did not develop or implement a procedure to monitor access to agency financial information by BPD or Oracle Corporation staff and contractors. As a result, increased risk exists that contractors or other users with privileged access could gain unauthorized access to or improperly use agency financial systems, applications, and information.

In addition, FHFA did not have a procedure to assess security reviews and plans of action and milestones that were conducted and documented by BPD or Oracle Corporation staff and contractors. While FHFA officials asserted that the agency randomly investigated some of the security

---

reviews and plans of action and milestones, the agency lacked a documented process for reviewing BPD's and Oracle Corporation's compliance with FHFA requirements. As a result, FHFA may not have assurance that the contractors are fully complying with security requirements.

FHFA informed us that it has initiated or has actions planned to fully implement effective oversight of contractors' adherence to its information security program. Specifically, a procedure to monitor security control compliance is under development and FHFA expects it to be finalized in June 2010. However, until all key elements of its information security program are fully implemented, FHFA may not have assurance that its controls are appropriately designed and operating effectively.

---

## Conclusions

Securing the information systems and information on which FHFA depends to carry out its mission requires that the agency establish, implement, and reinforce policies, procedures, and guidance. The agency has implemented numerous logical and physical access controls to safeguard financial systems and information and has instituted key components of an information security program. However, deficiencies in logical and physical access controls unnecessarily increased risk to FHFA's systems and key activities of its information security program were either not fully implemented or were absent. Until the agency strengthens its logical access and physical access controls and fully implements an information security program that includes policies and procedures reflecting the current agency environment, increased risk exists that sensitive information and resources will not be sufficiently protected from inadvertent or deliberate misuse, improper disclosure, or destruction.

---

## Recommendations for Executive Action

To help strengthen access controls and other information system controls over key financial systems, information, and networks, we recommend that the Acting Director of the Federal Housing Finance Agency implement the following 16 recommendations for strengthening logical access controls, physical access controls, and the agency's information security program.

---

To improve logical access controls, we recommend that the Acting Director ensures FHFA:

- (1) maintains network access authorizations for every agency network user;
- (2) reviews current access to network files and directories containing confidential information and restricts access to personnel with an authorized need to access that information; and
- (3) continuously monitors use of privileged accounts on systems throughout the network so inadvertent or extended use of privileged access is promptly detected and removed.

To strengthen controls over physical access, we recommend that the Acting Director ensures FHFA:

- (4) secures areas that contain IT equipment and sensitive information;
- (5) completes sufficient physical security policies to address protection of agency assets, including incident response, access authorizations, and environmental safety controls;
- (6) performs physical security risk assessments at key facilities;
- (7) develops, documents, and implements monitoring procedures to ensure that physical access authorizations to secure areas containing sensitive computer resources, including server rooms and sensitive information, are current and controlled;
- (8) develops, documents, and implements monitoring procedures and installs appropriate equipment to ensure that FHFA can detect and respond to potential physical security incidents;
- (9) implements and enforces visitor control practices at all facilities;
- (10) increases employees' awareness of the need to enforce physical security safeguards; and

- 
- (11) secures and removes construction materials from telecommunications and electrical closets that support computer operations.

To improve its information security program, we recommend that the Acting Director ensures FHFA:

- (12) develops, documents, and implements procedures enforcing separation of incompatible duties among personnel;
- (13) finalizes, approves, and implements configuration management policies and procedures;
- (14) approves and tests continuity of operations and disaster recovery plans;
- (15) develops, documents, and implements procedures to monitor access to agency financial information by BPD and Oracle Corporation staff and contractors; and
- (16) develops, documents, and implements procedures to assess all security reviews and plans of action and milestones developed by BPD and Oracle Corporation staff and contractors.

---

## Agency Comments

In providing written comments (reprinted in app. II) on a draft of this report, the Acting Director of the Federal Housing Finance Agency stated that FHFA agreed with our findings and will strengthen controls to reduce risk in the areas where we identified control deficiencies. He also noted that FHFA has already addressed or is in the process of addressing all the recommendations to strengthen controls over key financial systems, information, and networks. Further, the Acting Director stated that the agency was moving forward to strengthen and complete implementation of its information security program.

This report contains recommendations to you. As you know, 31 U.S.C. sec. 720 requires the head of a federal agency to submit a written statement of the actions taken on our recommendations to the Senate Committee on Homeland Security and Governmental Affairs and to the House Committee on Oversight and Government Reform not later than 60 days from the date of the report and to the House and Senate Committees on Appropriations with the agency's first request for appropriations made more than 60 days after the date of this report. Because agency personnel serve as the



---

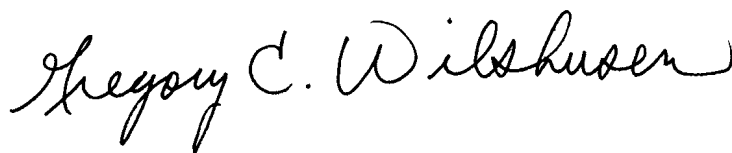
primary source of information on the status of recommendations, GAO requests that the agency also provide us with a copy of your agency's statement of action to serve as preliminary information on the status of open recommendations.

---

We are sending copies of this report to the Chairman and Ranking Member of the Senate Committee on Banking, Housing, and Urban Affairs; the Chairman and Ranking Member of the House Committee on Financial Services; the Chairman of the Federal Housing Finance Oversight Board; the Secretary of the Treasury; the Secretary of Housing and Urban Development; the Chairman of the Securities and Exchange Commission; the Director of the Office of Management and Budget; and other interested parties. In addition, this report will be available at no charge on the GAO Web site at <http://www.gao.gov>.

If you have any questions about this report or need assistance in addressing these issues, please contact Gregory C. Wilshusen at (202) 512-6244 or Dr. Nabajyoti Barkakati at (202) 512-4499 or by e-mail at [wilshuseng@gao.gov](mailto:wilshuseng@gao.gov) or [barkakatin@gao.gov](mailto:barkakatin@gao.gov). Contacts for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix III.

Sincerely yours,



Gregory C. Wilshusen  
Director, Information Security Issues



Dr. Nabajyoti Barkakati  
Director, Center for Technology and Engineering

---

# Appendix I: Objective, Scope, and Methodology

---

The objective of our review was to determine whether controls over key financial systems were effective in ensuring the confidentiality, integrity, and availability of financial information. This review was performed in connection with our audit of the Federal Housing Finance Agency's (FHFA) financial statements for the purpose of supporting our opinion on internal controls over the preparation of those statements.

To determine whether controls over key financial systems were effective, we tested information security controls at FHFA. We concentrated our evaluation primarily on threats focused on critical applications and their general support systems that directly or indirectly support the processing of material transactions that are reflected in the agency's financial statements. Our evaluation was based on our *Federal Information System Controls Audit Manual*, which contains guidance for reviewing information systems.

Using National Institute of Standards and Technology guidance, and FHFA's policies, procedures, practices, and standards, we evaluated controls by

- analyzing network and system share authorizations for agency network users;
- inspecting key devices to determine whether critical patches had been installed or were up-to-date;
- visiting the agency's three office buildings in Washington, D.C., on five different dates between July and September 2009 to observe and test physical access controls to determine if computer facilities and resources were being protected from inappropriate access by unauthorized individuals; and
- examining access responsibilities to determine whether incompatible functions were segregated among different individuals.

Using the requirements identified by the Federal Information Security Management Act, which established key elements for an effective agencywide information security program, we evaluated FHFA's implementation of its security program by

- analyzing agency policies, procedures, practices, and technical standards to determine whether sufficient guidance was provided to personnel responsible for securing information and information systems;

- analyzing security plans to determine if management, operational, and technical controls were planned or in place and that security plans were updated;
- analyzing test plans and test results for key agency systems to determine whether management, operational, and technical controls were based on risk and tested at least annually;
- examining contingency plans for key agency systems to determine whether those plans had been tested or updated; and
- analyzing FHFA's risk assessment process and risk assessments for key agency systems to determine whether risks and threats were documented.

We also reviewed or analyzed our previous reports and reports from the Department of the Treasury Office of Inspector General; and discussed with key security representatives and management officials whether information security controls were adequately designed, in place, and operating effectively.

We performed our work at FHFA facilities in Washington, D.C., and at financial application servicing and commercial hosting facilities in Parkersburg, West Virginia, and Austin, Texas. The work was conducted from February 2009 to April 2010 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

# Appendix II: Comments from the Federal Housing Finance Agency



FEDERAL HOUSING FINANCE AGENCY  
Office of the Director

April 16, 2010

Mr. Gregory C. Wilshusen  
Director, Information Security Issues  
Dr. Nabajyoti Barkakati  
Director, Center for Technology and Engineering  
Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

Dear Mr. Wilshusen and Dr. Barkakati:

Thank you for the opportunity to respond to the Government Accountability Office's (GAO) draft audit report titled "Information Security: Opportunities Exist for the Federal Housing Finance Agency (FHFA) to Improve Controls" (GAO-10-528), dated April 2010. I would like to personally compliment your staff for the thoroughness and professionalism with which they conducted the information security controls assessment during the FY 2009 Financial Statements Audit of FHFA.


Fiscal year 2009 was a tremendously challenging year for FHFA. In addition to the Agency's focus on stabilizing the housing market in the midst of financial market turmoil, FHFA was also creating the infrastructure for a new agency, including a new financial accounting system, new policies and procedures, and new internal controls. I am pleased that GAO found FHFA's fiscal year 2009 financial statements were fairly presented in all material respects and that FHFA had effective internal control over financial reporting.

During the course of the FY 2009 financial statement audit, GAO identified control deficiencies in our information security program that, while not considered significant for financial reporting purposes, subjected the agency to increased risk of unauthorized disclosure, modification or destruction of sensitive and financial information. We agree with these findings and will strengthen our controls to reduce risk in these areas. We have either already complied with, or are in the process of complying with, all of GAO's recommendations to strengthen controls over key financial systems, information, and networks.

As pointed out in the report, FHFA made important progress in developing and documenting elements of our information security program, but we had not yet fully implemented our agency wide information security program. We are moving forward expeditiously to strengthen and complete implementation of FHFA's information security program.

If you have any questions relating to our response, please contact Kevin Winkler, Chief Information Officer, at (202) 414-3769, or Mark Kinsey, Chief Financial Officer, at (202) 414-3811.

Yours truly,

  
Edward J. DeMarco  
Acting Director

1700 G Street, N.W., Washington, D.C. 20552-0003 • 202-414-3800 • 202-414-3823 (fax)

---

# Appendix III: GAO Contacts and Staff Acknowledgments

---

## GAO Contacts

Gregory C. Wilshusen, (202) 512-6244 or [wilshuseng@gao.gov](mailto:wilshuseng@gao.gov)

Dr. Nabajyoti Barkakati, (202) 512-4499 or [barkakatin@gao.gov](mailto:barkakatin@gao.gov)

---

## Staff Acknowledgments

In addition to the individuals named above, Charles Vrabel (Assistant Director), Edward Alexander (Assistant Director), Angela Bell, Bradley Becker, Debra Conner, Kirk Daubenspeck, Sharhonda Deloach, Rebecca Eyler, Rosanna Guerrero, Kevin Metcalfe, Eugene Stevens IV, Michael Stevens, and Christopher Warweg made key contributions to this report.

---

## GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

---

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site ([www.gao.gov](http://www.gao.gov)). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted Products, go to [www.gao.gov](http://www.gao.gov) and select "E-mail Updates."

---

## Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site [www.gao.gov/fraudnet/fraudnet.htm](http://www.gao.gov/fraudnet/fraudnet.htm)

E-mail [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Ralph Dawn, Managing Director, [dawnr@gao.gov](mailto:dawnr@gao.gov), (202) 512-4400  
U.S. Government Accountability Office, 441 G Street NW, Room 7125  
Washington, DC 20548

---

## Public Affairs

Chuck Young, Managing Director, [youngc1@gao.gov](mailto:youngc1@gao.gov), (202) 512-4800  
U.S. Government Accountability Office, 441 G Street NW, Room 7149  
Washington, DC 20548

