United States Government Accountability Office

GAO

Report to the Chairman, Board of Governors of the Federal Reserve System

August 2006

INFORMATION SECURITY

Federal Reserve Needs to Address Treasury Auction Systems

GAO-06-659

August 2006

INFORMATION SECURITY

Federal Reserve Needs to Address Treasury Auction Systems

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-06-659, a report to the Chairman, Board of Governors of the Federal Reserve System

Why GAO Did This Study

The Federal Reserve System's Federal Reserve Banks (FRB) serve as fiscal agents of the U.S. government when they are directed to do so by the Secretary of the Treasury. In this capacity, the FRBs operate and maintain several mainframe and distributed-based systems—including the systems that support the Department of the Treasury's auctions of marketable securities—on behalf of the department's Bureau of the Public Debt (BPD). Effective security controls over these systems are essential to ensure that sensitive and financial information is adequately protected from inadvertent or deliberate misuse, disclosure, or destruction.

In support of its audit of BPD's fiscal year 2005 Schedule of Federal Debt, GAO assessed the effectiveness of information system controls in protecting financial and sensitive auction information on key mainframe and distributed-based systems that the FRBs maintain and operate for BPD. To do this, GAO observed and tested FRBs' security controls.

What GAO Recommends

GAO is recommending that the Chairman, Board of Governors, establish an effective management structure for information security activities and a test environment for auction systems. In written comments on a draft of this report, the Federal Reserve generally agreed with the report and described actions to correct the identified weaknesses.
www.gao.gov/cgi-bin/getrpt?GAO-06-659.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

In general, the FRBs had implemented effective information system controls over the mainframe applications they maintain and operate for BPD in support of Treasury's auctions and financial reporting. On the distributed-based systems and supporting network environment used for Treasury auctions, however, they had not fully implemented information system controls to protect the confidentiality, integrity, and availability of sensitive and financial information. The FRBs did not consistently (1) identify and authenticate users to prevent unauthorized access; (2) enforce the principle of least privilege to ensure that access was authorized only when necessary and appropriate; (3) implement adequate boundary protections to limit connectivity to systems that process BPD business; (4) apply strong encryption technologies to protect sensitive data both in storage and on its networks; (5) log, audit, or monitor security-related events; and (6) maintain secure configurations on servers and workstations.

Without consistent application of these controls, the auction information and computing resources for key distributed-based auction systems remain at increased risk of unauthorized and possibly undetected use, modification, destruction, and disclosure. Other FRB applications that share common network resources may also be at increased risk.

Contributing to these weaknesses in information system controls were the Federal Reserve's lack of (1) an effective management structure for coordinating, communicating, and overseeing information security activities across bank organizational boundaries and (2) an adequate environment in which to sufficiently test the security of its auction applications.

Contents

Letter 1

Results in Brief 2
Background 3
Objective, Scope, and Methodology 6
Security of Treasury Auction Systems Needs to Be Addressed 8
Conclusions 16
Recommendations for Executive Action 16
Agency Comments 17

Appendixes

Appendix I: Comments from the Federal Reserve 19

Appendix II: GAO Contacts and Staff Acknowledgments 21

Figure

Figure 1: One FRB System Managed by Multiple Information Technology Groups 14

Abbreviations

BPD	Bureau of the Public Debt
FRB	Federal Reserve Bank
FRIT	Federal Reserve Information Technology
IT	information technology

G A O
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, D.C. 20548

August 30, 2006

The Honorable Ben Bernanke
Chairman, Board of Governors of the Federal
Reserve System

Dear Mr. Bernanke:

As the central bank of the United States, the Federal Reserve System has an important role in ensuring the safety and soundness of the nation's banking and financial system. The Federal Reserve System's Federal Reserve Banks (FRB) serve as fiscal agents of the U.S. government when directed to do so by the Secretary of the Treasury. In this capacity, the FRBs operate and maintain several mainframe and distributed-based systems[1] on behalf of the Department of Treasury's Bureau of the Public Debt (BPD). Effective controls[2] over these information systems are essential to ensuring that sensitive and financial information is adequately protected from inadvertent or deliberate misuse, disclosure, or destruction.

As you know, Treasury is authorized by Congress to borrow money on the credit of the United States to pay off maturing debt and raise the cash needed to operate the federal government. Within Treasury, BPD is the organizational entity designated to carry out this responsibility.[3] It does so by selling securities at auctions conducted electronically through one of its internal offices and through the FRBs and their branches. BPD has delegated the responsibility for processing auction transactions to the

[1]Distributed-based systems consist of a number of components, which are themselves computer systems. The components are connected by a communications medium, usually a sophisticated network. Applications execute by using a number of processes in different component systems. These processes communicate and interact to achieve productive work within the application.

[2]Information system controls include general and application controls. Both general and application controls must be effective to help ensure the confidentiality, integrity, and availability of critical or sensitive automated information. General controls affect the overall effectiveness of the security of computer operations as opposed to being unique to any specific computer application. These controls include logical access controls, specifically, those controls that prevent or detect unauthorized access to sensitive data and programs that are stored, processed, and transmitted electronically. Application controls relate directly to individual computer applications that are used to perform specific functions or process transactions.

[3]BPD's responsibility includes issuing and redeeming debt instruments, paying interest to investors, and accounting for the resulting debt.

FRBs. Acting in this capacity, various FRB information technology (IT) support organizations maintain and operate automated auction systems on BPD's behalf. These systems receive bids, calculate the auction results, and generate notices and receipts of electronic tenders and awarded bids.

In support of our audit of BPD's fiscal year 2005 Schedule of Federal Debt,[4] we assessed the effectiveness of information system controls over key financial systems that the FRBs maintain and operate on behalf of BPD. These systems included mainframe applications that support Treasury auctions and financial reporting, distributed-based systems that support Treasury auctions, and networks that interconnect those systems. In forming an opinion on BPD's internal control relevant to the Schedule of Federal Debt, we considered the results of our review of information security controls at BPD and the FRBs relevant to the Schedule of Federal Debt.[5] Our review also considered applicable compensating and management reconciliation controls at BPD.

This report discusses the effectiveness of information system controls in ensuring the confidentiality, integrity, and availability of Treasury's financial and sensitive auction information on mainframe and distributed-based systems that the FRBs maintain and operate on behalf of BPD and that are relevant to the Schedule of Federal Debt.

Results in Brief

The FRBs had generally implemented effective controls over their mainframe applications that they maintain and operate on behalf of BPD in support of Treasury's financial reporting. However, the FRBs had not effectively implemented information system controls to protect the confidentiality, integrity, and availability of sensitive data and computing resources for the distributed-based systems and the supporting network environment relevant to Treasury auctions. Specifically, the FRBs did not

[4]GAO, *Financial Audit: Bureau of the Public Debt's Fiscal Years 2005 and 2004 Schedules of Federal Debt*, GAO-06-169 (Washington, D.C.: Nov. 7, 2005).

[5]In that review, we opined that BPD maintained, in all material respects, effective internal control relevant to the Schedule of Federal Debt related to financial reporting and compliance with applicable laws and regulations, as of September 30, 2005. We found matters involving information security controls that did not adversely affect the audit opinion on internal control. BPD mitigates the potential effect of such issues with physical security measures, with a program of monitoring user and system activity on systems that BPD operates and maintains, and by compensating management and reconciliation controls.

consistently (1) identify and authenticate users to prevent unauthorized access; (2) enforce the principle of least privilege to ensure that authorized access was necessary and appropriate; (3) implement adequate boundary protections to limit connectivity to systems that process BPD business; (4) apply strong encryption technologies to protect sensitive data in storage and on its networks; (5) log, audit, or monitor security-related events; and (6) maintain secure configurations on servers and workstations.

As a result, auction information and computing resources for key distributed-based auction systems that the FRBs maintain and operate on behalf of BPD are at an increased risk of unauthorized and possibly undetected use, modification, destruction, and disclosure. Furthermore, other FRB applications that share common network resources with the distributed-based systems may face similar risks.

These information system control weaknesses existed, in part, because the FRBs did not have (1) an effective management structure for coordinating, communicating, and overseeing information security activities across bank organizational boundaries and (2) an adequate environment in which to sufficiently test the auction applications.

We are making recommendations to you to establish an effective management structure for implementing key information security activities and a test environment for auction systems.

We are also making additional recommendations in a separate report with limited distribution. These recommendations address actions needed to correct the specific information security weaknesses in the distributed-based systems and network infrastructure.

In providing written comments on a draft of this report (reprinted in app. I), the Director, Division of Reserve Bank Operations and Payment Systems of the Federal Reserve System, described completed, ongoing, and planned corrective actions to address the weaknesses identified in the report.

Background

For any organization that depends on information systems to carry out its mission, protecting those systems that support critical operations and infrastructures is of paramount importance. Without proper safeguards, the speed and accessibility that create the enormous benefits of the computer age may allow individuals and groups with malicious intent to gain

unauthorized access to systems and use this access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other sites.

Concerns about attacks from individuals and groups, including terrorists, 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, the steady advance in the sophistication and effectiveness of attack technology, and the dire warnings of new and more destructive attacks to come. Given these threats, the security of computer-supported federal operations are at risk and place a variety of critical operations at risk of disruption, fraud, and inappropriate disclosure. We have designated information security as a governmentwide high-risk area since 1997[6]—a designation that remains today.[7]

To address these concerns, Congress enacted the Federal Information Security Management Act of 2002[8] to strengthen the security of information collected or maintained and information systems used or operated by federal agencies, or by a contractor or other organization on behalf of a federal agency. The act provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. The act requires each agency to develop, document, and implement an agencywide information security program for the information and systems that support the operations of the agency as well as information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

Structure of the Federal Reserve System

Established by the Federal Reserve Act of 1913, the Federal Reserve System consists of a 7-member Board of Governors with headquarters in Washington, D.C.; 12 Reserve Districts, each with its own FRB located in a major city in the United States; and 25 bank branches. The Federal Reserve System differs from other entities established to carry out public purposes

[6]GAO, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: February 1997).

[7]GAO, *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: January 2005).

[8]Enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 166 Stat. 2946 (Dec. 17, 2002).

in that it is part public and part private. Although the Board is a government agency, the banks are not. Also, the Federal Reserve System structure does not follow the familiar "top-down" hierarchy, with all policymaking authorities centralized in Washington, D.C. The Board and the FRBs have shared responsibilities and policymaking authority in many areas of operation.

The FRBs Serve as Treasury Fiscal Agents

The FRBs play a significant role in the processing of marketable Treasury securities. As fiscal agents of Treasury, the FRBs receive bids, issue securities to awarded bidders, collect payments on behalf of Treasury, and make interest and redemption payments from Treasury's account to the accounts of security holders. During fiscal year 2005, the FRBs processed debt held by the public of about $4.5 trillion in issuances, about $4.2 trillion in redemptions, and about $128 billion in interest payments. Certain FRBs also provide IT services in support of Treasury auctions, operating and maintaining the Treasury mainframe auction application in which bid submissions are recorded and the auction results calculated.

In addition to the Treasury mainframe auction application, the FRBs also operate and maintain two Treasury distributed-based auction applications. These applications provide the user interface to the mainframe auction application through the Federal Reserve networks. One of the distributed-based auction applications serves approximately 670 users, allowing them to participate in public (primarily noncompetitive) auctions via the Internet. The other distributed-based auction application serves 22 primary broker/dealers[9] for competitive auctions who connect to it via workstations installed in the dealers' offices by the FRBs. One nonprimary broker/dealer is allowed to access this distributed-based auction application via the Internet on a trial basis. These distributed-based auction applications transmit information on the tenders/bids, including the name of the submitter, the par amount of securities being tendered or awarded, the discount rate being tendered or awarded, and the clearing bank. Multiple Federal Reserve organizations are involved in the operation and maintenance of these applications, including the Federal Reserve

[9]As of January 2006, there were 22 primary broker/dealers who serve as trading counterparties for the Federal Reserve in the Treasury securities market, designated by FRB New York on the basis of their ability to (1) make reasonably good markets in their trading relationships with the Federal Reserve trading desk; (2) participate meaningfully in Treasury auctions; and (3) market information and analysis that may be useful to the Federal Reserve in the formulation and implementation of monetary policy.

Information Technology (FRIT)—the organization that provides entitywide IT support services for the Federal Reserve System.

Other systems supporting Treasury financial reporting are mainframe-based applications and are used to record securities purchased by financial institutions, provide an automated system for investors to buy securities directly from Treasury and manage their Treasury securities portfolios, and monitor and track all cash received and disbursed for debt transactions that the FRBs process.

Objective, Scope, and Methodology

The objective of our review was to assess the effectiveness of information system controls in ensuring the confidentiality, integrity, and availability of Treasury's financial and sensitive auction information on key mainframe and distributed-based systems that the FRBs maintain and operate on behalf of BPD and that are relevant to the Schedule of Federal Debt. Our assessment included a review of the supporting network infrastructure that interconnects the mainframe and distributed-based systems.

To accomplish this objective, we used elements of our *Federal Information System Controls Audit Manual*[10] to evaluate information system controls within the FRB control environment. We concentrated our efforts primarily on the evaluation of logical access controls over the FRBs' distributed-based auction applications because of their recent implementation and the Federal Reserve network infrastructure that supports these applications. To evaluate these applications, we reviewed information system controls over network resources used by the applications and focused on the following control domain areas: identification and authentication; authorization; boundary protection; cryptography; logging, auditing, and monitoring; and configuration management and assurance. Our review included observations of Treasury auction operations and an examination of

- automated programs related to the auction process;
- system data collected by FRB employees in our presence and at our direction;

[10]GAO, *Federal Information System Controls Audit Manual*, GAO/AIMD-12.19.6 (Washington, D.C.: January 1999).

- system and infrastructure documentation;
- source code for the distributed-based auction applications; and
- configuration files of firewalls, routers, and switches.

We also examined policy and procedural documentation for the FRBs' distributed computing security and network security, interviewed information technology managers and staff, and familiarized ourselves with the operations of the general auditors and with the results of their recent work applicable to our audit.

In addition, we performed limited application controls testing over the Treasury mainframe auction application and other key mainframe applications that support Treasury's financial reporting. Specifically, we evaluated application controls associated with access (segregation of duties, least privilege, and identification and authentication); controls over master data; transaction data input (data validation and edit checks); transaction data processing (data integrity and logs); and transaction data output (output reconciliation and review). To evaluate the effectiveness of these controls, we obtained system configuration information using GAO-prepared analytical tools run by FRB IT staff, and verified critical operating system logging and access control information for relevant system configurations. Also, using GAO-prepared scripts, we obtained information on operating system utilities with assistance from FRB IT staff.

We discussed with officials from the staff of the Board of Governors and key Federal Reserve information security representatives and officials whether information security controls were in place, adequately designed, and operating effectively. We also discussed with these individuals the results of our review.

We performed our work at the FRBs that operate and maintain the mainframe and distributed-based financial reporting and auction applications we selected for review. We performed our work from March 2005 through May 2006 in accordance with generally accepted government auditing standards.

Security of Treasury Auction Systems Needs to Be Addressed

Although the FRBs established and implemented many controls to protect the mainframe applications that they maintain and operate on behalf of BPD, they did not consistently implement controls to prevent, limit, or detect unauthorized access to sensitive data and computing resources for the distributed-based systems and network environment that support Treasury auctions. As a result, increased risk exists that unauthorized and possibly undetected use, modification, destruction, and disclosure of certain sensitive auction information could occur. Furthermore, other FRB applications that share common network resources may also face increased risk.

These information system control weaknesses existed, in part, because the FRBs did not have (1) an effective management structure for coordinating, communicating, and overseeing information security activities across bank organizational boundaries and (2) an environment to sufficiently test the auction applications.

Mainframe Control Environment

The FRBs had generally implemented effective information system controls for the mainframe applications that they operate and maintain on behalf of BPD in support of Treasury's auctions and financial reporting. Examples of these controls include multiple layers of procedural and technical controls over mainframe systems, effective isolation of mainframe systems having different control requirements, and continuous independent auditing of mainframe technical controls. In addition, FRIT upgrades the software for the mainframe systems on an annual schedule. Each year, a new logical partition of the mainframe is created with the upgraded operating system and vendor-supplied software. This logical partition is then tested in a defined process, which is subject to an annual audit, and there is continuous monitoring of the production logical partitions.

Distributed-Based Systems and Supporting Network Environment

Although the mainframe control environment was generally effective, the FRBs had not effectively implemented information system controls for the distributed-based systems and supporting network environment relevant to Treasury auctions. More specifically, the FRBs did not consistently (1) identify and authenticate users to prevent unauthorized access; (2) enforce the principle of least privilege to ensure that authorized access was necessary and appropriate; (3) implement adequate boundary protections to limit connectivity to systems that process BPD business; (4) apply strong

encryption technologies to protect sensitive data in storage and on the Federal Reserve networks; (5) log, audit, or monitor security-related events; and (6) maintain secure configurations on servers and workstations.

Identification and Authentication

A computer system must be able to identify and differentiate among users so that activities on the system can be linked to specific individuals. When an organization assigns unique user accounts to specific users, the system distinguishes one user from another—a process called identification. The system also must establish the validity of a user's claimed identity through some means of authentication, such as a password, that is known only to its owner. The combination of identification and authentication—such as user account/password combinations—provides the basis for establishing individual accountability and for controlling access to the system. The National Institute of Standards and Technology states that information systems should employ multifactor authentication, such as a combination of passwords, tokens, and biometrics.

The FRBs did not adequately identify and authenticate users. For example, due to the weak design of password reset functionality for one of the distributed-based auction applications, anyone on the Internet could potentially change the password for a user in the application by having only his or her userID. Recognizing the severity of this vulnerability, the FRBs took steps to immediately correct this weakness.

The FRBs also designed and implemented the distributed-based auction applications to only rely on one means of authentication, rather than a combination of authentication factors for controlling access. Furthermore, the FRBs did not replace a well-known vendor-supplied password on one of their systems, thereby increasing the risk that an unauthorized individual could guess the password and gain access to the system.

Authorization

Authorization is the process of granting or denying access rights and privileges to a protected resource, such as a network, system, application, function, or file. A key component of granting or denying access rights is the concept of "least privilege." Least privilege is a basic underlying principle for securing computer resources and data. The term means that users are granted only those access rights and permissions that they need to perform their official duties. To restrict legitimate users' access to only those programs and files that 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 are associated with a particular file or directory and regulate which users can access them and the extent of that access. To avoid unintentionally giving users unnecessary access to sensitive files and directories, an organization must give careful consideration to its assignment of rights and permissions.

The FRBs did not implement sufficient authorization controls to limit user access to distributed-based computer resources. The distributed-based auction applications had excessive database privileges that were granted explicitly as well as inherited through permissions given to all users. As a result, malicious users could use these excessive privileges to exploit other vulnerabilities in the applications. In addition, the FRBs had granted users administrative privileges on their workstations, even though most users did not require this level of access. Granting unnecessary access privileges increases the risk that a workstation could be successfully compromised and then used to attack other FRB resources. As a result, the unnecessary level of access granted to computer resources provides opportunities for individuals to circumvent security controls to deliberately or inadvertently read, modify, or delete critical or sensitive information.

Boundary Protection

Boundary protections demarcate a logical or physical boundary between protected information and systems and unknown users. Organizations physically allocate publicly accessible information system components to subnetworks with separate, physical network interfaces, and prevent public access into their internal networks, except as authorized. Unnecessary connectivity to an organization's network not only increases the number of access paths that must be managed and the complexity of the task, but increases the risk in a shared environment.

The FRBs did not consistently implement adequate boundary protections to limit connectivity to applications in the shared network environment. These applications include those that the FRBs operate and maintain on behalf of BPD and other FRB internal applications and systems that serve a variety of business areas with differing security requirements. In addition, the internal network was not segregated to restrict access to internal systems, and management of network devices and applications was conducted "in-band."[11] These practices increase the risk that individuals

[11]"In-band management" refers to using the same logical and physical network as normal applications and user communications instead of separating this traffic.

could disrupt or gain unauthorized access to sensitive auction data and other Federal Reserve computing resources.

In some cases, the FRBs implemented effective boundary protection controls. For example, the remote access system used Federal Information Processing Standard compliant tokens for authentication and enforced a restriction that prevented simultaneous communication with the internal Federal Reserve network and the Internet.

Cryptography

Cryptography underlies many of the mechanisms used to enforce the confidentiality and integrity of critical and sensitive information. Encryption—one type of cryptography—is the process of converting readable or plaintext information into unreadable or ciphertext information using a special value known as a key and a mathematical process known as an algorithm. The strength of a key and an algorithm is determined by their length and complexity—the longer and more complex they are, the stronger they are.

The FRBs did not appropriately apply strong encryption technologies to sensitive data and network traffic. Weak encryption algorithms, such as the user's session information and application configuration files, were used to protect sensitive data in one of the distributed-based auction applications. Also, a weak encryption format was used to store and transmit certain passwords. These weaknesses could allow an attacker to view data and use that knowledge to gain access to sensitive information, including auction data.

Logging, Auditing, and Monitoring

Determining what, when, and by whom specific actions were taken on a system is crucial to establishing individual accountability, investigating security violations, and monitoring compliance with security policies. Organizations accomplish this by implementing system or security software that provides an audit trail for determining the source of a transaction or attempted transaction and for monitoring users' activities.

How organizations configure the system or security software determines what system activity data are recorded into system logs and the nature and extent of the audit trail information that results. Without sufficient auditing and monitoring, organizations increase the risk that they may not detect unauthorized activities or policy violations. Furthermore, the National Institute of Standards and Technology guidance states that organizations should deploy centralized servers and configure devices to send duplicates of their log entries to the centralized servers.

The FRBs did not sufficiently log, audit, or monitor events related to the distributed-based auction application process. For example, the intrusion detection system had not been customized to detect any abnormal communication among application components that might indicate an attack was in progress. In addition, no centralized logging was performed for certain servers we examined. As a result, there was a higher risk that unauthorized system activity would not be detected in a timely manner.

Configuration Management and Assurance

To protect an organization's information, it is important to ensure that only authorized application programs are placed in operation. This process, known as configuration management, is accomplished by instituting policies, procedures, and techniques to help ensure that all programs and program modifications are properly authorized, tested, and approved.

Patch management, a component of configuration management, is an important element in mitigating the risks associated with software vulnerabilities. When a software vulnerability is discovered, the software vendor may develop and distribute a patch or work-around to mitigate the vulnerability. Up-to-date patch installation can help mitigate vulnerabilities associated with flaws in software code that could be exploited to cause significant damage, ranging from Web-site defacement to the loss of control of entire systems, thereby enabling malicious individuals to read, modify, or delete sensitive information; disrupt operations; or launch attacks against other organizations' systems. Configuration assurance is the process of verifying the correctness of the security settings on hosts, applications, and networks and maintaining operations in a secure fashion.

The FRBs did not maintain secure configurations on the distributed-based auction application servers and workstations we reviewed. Key servers and FRB workstations were missing patches that could prevent an attacker from gaining remote access. In addition, the FRBs were running a database management system and network devices that were no longer supported by the vendor. Unsupported products greatly increase the risk of security breaches, since the vendor often does not provide patches for known vulnerabilities. As a result of these weaknesses, the risk is increased of a successful attack and compromise of the related auction process.

Certain Information Security Practices Not Implemented

The previously mentioned information system control weaknesses existed, in part, because the FRBs did not have (1) an effective management structure for coordinating, communicating, and overseeing information

security activities across bank organizational boundaries and (2) an environment to sufficiently test the auction applications.

Effective Management Structure Not Established

Implementing effective information security management practices across the enterprise is essential to ensuring that controls over information and information systems work effectively on a continuing basis, as described in our May 1998 study of security management best practices.[12] An important factor in implementing effective practices is linking them in a cycle of activity that helps to ensure that information security policies address current risks on an ongoing basis. An effective management structure is the starting point for coordinating and communicating the continuous cycle of information security activities, while providing guidance and oversight for the security of the entity as a whole. One mechanism organizations can adopt to achieve effective coordination and communication, particularly in organizations where information security management is decentralized, is to establish a central security management office or group to serve as a facilitator to individual business units and senior management. A central security group serves as a locus of knowledge and expertise on information security and coordinates agencywide security-related activities. This group is also accessible to security specialists at the various organizational elements within the agency.

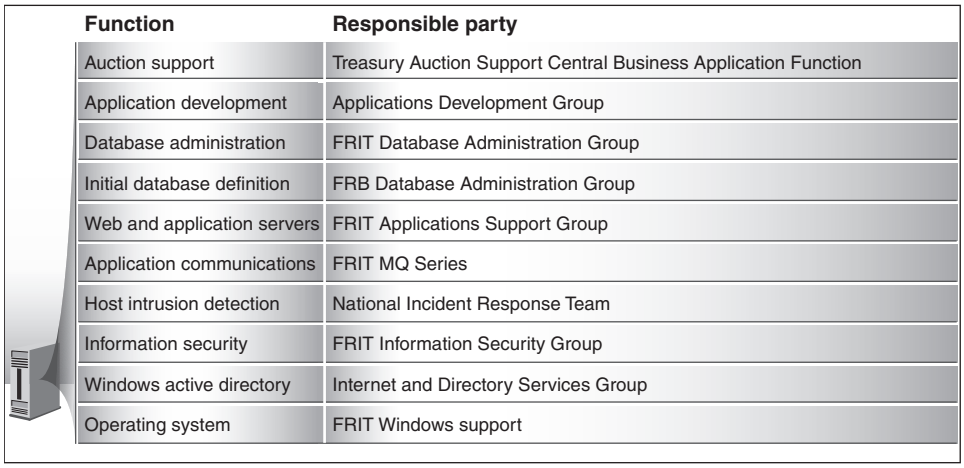
Such a management structure is especially important to manage the inherent risks associated with a highly distributed, interconnected network-based computing environment and to help ensure that weaknesses in one system do not place the entire entity's information assets at undue risk. In addition, as part of this management structure, clearly defined roles and responsibilities for all security staff should be established and coordination of responsibilities among individual security staff should be developed and communicated to ensure that, collectively, information security activities are effective.

The FRBs did not have an effective management structure for coordinating, communicating, and overseeing their decentralized information security management activities that support Treasury auction systems and the supporting network infrastructure. Each bank operates independently and autonomously of one another, yet they share many of the same systems and computing resources. Because the FRBs did not have an effective

[12]GAO, *Executive Guide: Information Security Management–Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

information security management structure over the distributed-based systems, information security activities were not adequately coordinated among the banks and with the various IT groups involved in providing IT support services, including FRIT—the organization that provides entitywide IT support services. For example, information management activities associated with one of the distributed-based auction systems was divided among 10 IT groups, as shown in figure 1.

Figure 1: One FRB System Managed by Multiple Information Technology Groups



Function	Responsible party
Auction support	Treasury Auction Support Central Business Application Function
Application development	Applications Development Group
Database administration	FRIT Database Administration Group
Initial database definition	FRB Database Administration Group
Web and application servers	FRIT Applications Support Group
Application communications	FRIT MQ Series
Host intrusion detection	National Incident Response Team
Information security	FRIT Information Security Group
Windows active directory	Internet and Directory Services Group
Operating system	FRIT Windows support

Source: GAO analysis of Federal Reserve data.

In addition, no IT group was responsible for coordinating and communicating enterprisewide security operations support or oversight services. Consequently, the various organizations responsible for implementing information security did not have a good understanding or adequate visibility of the activities that other groups performed, nor did they always make appropriate decisions about information security for the network environment as a whole. As a result, there was no enterprisewide view of information security, and decisions regarding information security activities were not always optimal or based on a full understanding of the shared network environment supporting the Treasury auction process. For example,

- one IT group responsible for database operations made information security decisions regarding the distributed-based auction applications

on the concept that they were operating in a "trusted network," which resulted in the omission of controls that should have been in place;

- one IT group made decisions about the operations and maintenance of the distributed-based auction applications without full or accurate knowledge of the relevant computing environment;

- no IT group had responsibility for making a decision to upgrade the distributed-based auction database product, although all concerned agreed that an upgrade was needed; and

- servers that support the distributed-based auction applications were supposed to be identical to ensure real-time continuity of operations, but our testing showed that, as implemented, they were not identical.

The Federal Reserve recognizes that a need exists for comprehensive approaches to managing information security, and that the management structure and processes that served its mainframe-centric environment in the past are not adequate for the distributed, interconnected environment supporting its various lines of business today. The Federal Reserve has an initiative under way to establish an information security architecture framework that is intended to integrate enterprise security activities, including enterprise access management, domain boundary, data security, configuration management, and information assurance. If effectively implemented, this initiative could provide the FRBs with an enterprisewide operational and technological view of its computing environment, including the interdependencies and interrelationships across the entity's business operations and underlying IT infrastructure and applications that support these operations.

However, until a more comprehensive and enterprisewide approach to security management is adopted, the FRB organizations that support Treasury auction systems will be limited in their ability to ensure the confidentiality, integrity, and availability of certain sensitive auction information and other resources for systems that they maintain and operate.

Test Environment for Auction Systems Lacking

The FRBs did not have a test environment to evaluate system changes and enhancements to the distributed-based auction applications, which limited the rigor of the testing that could be performed. A separate test environment that models the production environment is critical to ensuring that systems and system enhancements are adequately tested and do not

adversely affect production.[13] However, the FRBs did not have an isolated testing area that was functionally separate from the production network infrastructure and other FRB business applications. As a result, some application security testing was performed during very limited scheduled outages of the production systems involved, and some test procedures were never performed because the risk to production systems could not be effectively mitigated.

Conclusions

Although the FRBs have implemented many controls to protect the mainframe information systems that they maintain on behalf of BPD relevant to the Schedule of Federal Debt, information security control weaknesses related to the distributed-based auction systems and supporting network environment exist at the Federal Reserve that place certain sensitive auction information at risk. The weaknesses in identification and authentication; authorization; boundary protection; cryptography; logging, auditing, and monitoring; and configuration management and assurance affect not only the distributed-based auction systems but also could affect other FRB systems residing in the shared network environment. With control over and responsibility for Treasury's auction information systems spread across the FRBs, an effective management structure for coordinating, communicating, and overseeing information security activities across bank organizational boundaries becomes even more important. In addition, more robust testing of security controls over the auction applications is imperative to help provide more timely detection of vulnerabilities. Until the Federal Reserve takes steps to mitigate these weaknesses, it has increased risk that sensitive auction data would not be adequately protected against unauthorized disclosure, modification, or destruction.

Recommendations for Executive Action

To help strengthen the FRBs' information security over key distributed-based auction systems, we recommend that you take the following two steps:

- establish a management structure that ensures decentralized information security activities are effective and

[13]Dustin, Elfriede. *Effective Software Testing* (Boston, MA: Addison-Wesley, Pearson-Education, Inc., 2003).

- implement an application test environment for the auction systems.

We are also making additional recommendations in a separate report with limited distribution. These recommendations consist of actions to be taken to correct the specific information security weaknesses we identified that are related to identification and authentication; authorization; boundary protection; cryptography; logging, auditing, and monitoring; and configuration management and assurance.

Agency Comments

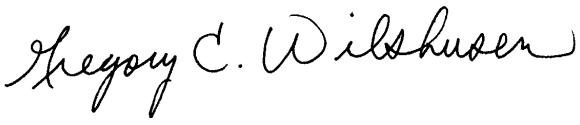
In providing written comments on a draft of this report (reprinted in app. I), the Director, Division of Reserve Bank Operations and Payment Systems of the Federal Reserve System, generally agreed with the contents of the draft report and stated that the Federal Reserve has already taken corrective actions to remedy many of the reported findings and will continue to apply its risk-based assessment framework to determine appropriate information security controls or compensating measures to address the remaining findings. The director also described completed, ongoing, and planned actions to address systemic and organizational issues that contributed to the report's findings, including actions to improve the Federal Reserve's ability to coordinate and oversee its operational and technical environments and to replace its existing auction applications and operational infrastructure. In addition, the director commented that the Federal Reserve and Treasury plan to validate the integrity of the new application and infrastructure at several points during the development of the application; a key aspect of this validation is to ensure that the findings in this report are addressed.

This report contains recommendations to you. As you know, 31 U.S.C. 720 requires that the head of a federal agency 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 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 Chairmen and Ranking Minority Members of the Senate Committee on Homeland Security and Governmental Affairs; the Subcommittee on Federal Financial Management, Government Information, and International Security, Senate Committee on Homeland Security and Governmental Affairs; and the Chairmen and Ranking Minority Members of the House Committee on Government Reform and the Subcommittee on Government Management, Finance, and Accountability, House Committee on Government Reform. In addition, we are sending copies to the Fiscal Assistant Secretary of the Treasury and the Deputy Director for Management of OMB. We will also make copies available to others upon request. In addition, this report will be available at no charge on the GAO Web site at http://www.gao.gov.

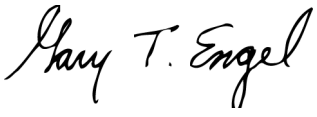
If you or your staff have any questions about this report, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, Keith A. Rhodes at (202) 512-6412 or rhodesk@gao.gov, or Gary T. Engel at (202) 512-8815 or engelg@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix II.

Sincerely yours,



Gregory C. Wilshusen
Director, Information Security Issues

Keith A. Rhodes
Chief Technologist



Gary T. Engel
Director, Financial Management and Assurance

Comments from the Federal Reserve

BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D.C. 20551

LOUISE L. ROSEMAN
DIRECTOR
DIVISION OF
RESERVE BANK OPERATIONS
AND PAYMENT SYSTEMS

August 10, 2006

Mr. Gregory C. Wilshusen
Director, Information Security Issues
Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Wilshusen:

On behalf of Chairman Bernanke, thank you for the opportunity to comment on the GAO's report titled *Information Security: Federal Reserve Needs to Address Treasury Auction Systems*. The GAO's audit of the Treasury auction systems was conducted as part of its review of the Bureau of the Public Debt's FY 2005 Schedules of Federal Debt. The report identified a number of weaknesses in Reserve Bank computer-based information security control environments in the distributed computing and network environments that support the Treasury auction processes. We have already taken corrective actions to remediate many of the findings in the report, and we will continue to apply our risk-based assessment framework to determine appropriate information security controls or compensating measures to address remaining findings.

The Reserve Banks are taking action to address systemic and organizational issues that contributed to the report's findings. We met with the GAO review team several times to discuss our plans to further strengthen our information security architecture and to correct the root causes of the findings so that we avoid recurring weakness in controls. The report recognizes that successful implementation of the strengthened architecture could improve our ability to manage our information security operational and technical environments. We have also taken actions to improve our ability to coordinate and oversee our complex IT systems effectively. The Reserve Banks recently realigned their information security governance structure and designated the Director of the Reserve Banks' Federal Reserve Information Technology organization (FRIT) as the focal point for enterprise-wide information security. All operational units within the Federal Reserve Banks are responsible for confirming compliance with established information security operational practices and information security policies and standards with the Director of FRIT. As part of this realignment, FRIT established a new function, National Information Security Assurance (NISA), which is responsible for monitoring end-to-end information security compliance with security standards, including software currency, across the Federal Reserve. Further, NISA will maintain an aggregate view of information security risk across all risk management programs, including internal audit and external sources, such as the GAO.

Email: Louise.Roseman@frb.gov
Phone: (202) 452-2789 • Fax: (202) 452-2746

The Treasury auction applications reviewed in this report were developed starting in 1998 when web technology, tools, and development practices were substantially less evolved than those available today. While security methods for web-based applications have improved, so has the sophistication of criminals attempting to compromise them. The Treasury and the Federal Reserve are currently undertaking a significant development initiative to replace the existing applications and operational infrastructure by year-end 2007. The design of the new application and infrastructure is based on current sound practices that will ensure a well-managed and well-controlled operating environment. The Federal Reserve and Treasury plan to validate the integrity of the application and infrastructure at several points in the project using internal and external technical resources. A key aspect of this validation is ensuring the GAO's findings are addressed. The new auction applications will be operated within the Federal Reserve's strengthened information security architecture, and information security compliance will be monitored through our improved information security governance structure.

As your report notes, this review specifically focused on information security controls in the distributed computing and network environments supporting the Treasury auction process. The GAO's review did not consider the end-to-end risk control environment that would include management and business operational controls. This additional layer of control is critical to ensuring the integrity of the Schedules of Federal Debt. The information security vulnerabilities the GAO identified did not affect its opinion in its report titled *Financial Audit: Bureau of the Public Debt's Fiscal Years 2004 and 2005 Schedules of Federal Debt.* That report noted that effective internal controls over financial reporting and compliance with applicable laws and regulations were maintained. Although we consider the information security control vulnerabilities identified in the Treasury auction system report significant and warranting our serious attention, they should not be construed as allowing successful circumvention of Treasury auction management and business operational controls.

We appreciate the quality of the GAO technical review and the time taken by the review team to brief Federal Reserve and Treasury staff thoroughly on the results of the review. The GAO team has also contributed to our remediation efforts by consulting with various Federal Reserve technical and management staff on the technical details underlying the findings in the report.

Sincerely,

GAO Contacts and Staff Acknowledgments

GAO Contacts

Gregory C. Wilshusen, Director, Information Security Issues, (202) 512-6244

Keith A. Rhodes, Chief Technologist, (202) 512-6412

Gary T. Engel, Director, Financial Management and Assurance, (202) 512-8815

Staff Acknowledgments

In addition to the individuals named above, Ed Alexander, Lon Chin, Edward Glagola, David Hayes, Hal Lewis, Duc Ngo, Dawn Simpson, and Jenniffer Wilson, Assistant Directors, and Mark Canter, Dean Carpenter, Jason Carroll, West Coile, Debra Conner, Neil Doherty, Nancy Glover, Sharon Kittrell, Eugene Stevens, Henry Sutanto, Amos Tevelow, and Chris 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). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548