United States General Accounting Office

GAO

Report to Congressional Requesters

July 2003

# INFORMATION SECURITY

# Computer Controls over Key Treasury Internet Payment System


GAO-03-837

July 2003

# INFORMATION SECURITY

# Computer Controls over Key Treasury Internet Payment System

GAO Accountability • Integrity • Reliability

## Highlights

Highlights of GAO-03-837, a report to Congressional Requesters.

## Why GAO Did This Study

"Pay.gov" is an Internet portal sponsored and managed by the Department of the Treasury's Financial Management Service (FMS) and operated at three Federal Reserve facilities. Pay.gov is intended to allow the public to make certain non-income-tax-payments to the federal government securely over the Internet. FMS estimates that Pay.gov eventually could annually process 80 million transactions valued at $125 billion annually.

Because of the magnitude of transaction volume and dollar value envisioned for Pay.gov, GAO was asked to determine whether FMS (1) conducted a comprehensive security risk assessment and (2) implemented and documented appropriate security measures and controls for the system's protection.

## What GAO Recommends

GAO recommends that the Commissioner of FMS direct the Pay.gov program manager to implement a number of actions to strengthen security over Pay.gov.

The FMS Commissioner concurred with our recommendations and stated that FMS had taken action to correct almost all of the weaknesses that GAO identified and has plans to correct the remaining weaknesses.

www.gao.gov/cgi-bin/getrpt?GAO-03-837.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Robert F. Dacey at (202) 512-3317 or daceyr@gao.gov.

## What GAO Found

FMS had not fully assessed the risks associated with the Pay.gov initiative. Although the agency prepared a business risk assessment for the Pay.gov application, it had not fully assessed the risks associated with Pay.gov computing environment. Insufficiently assessing risks can lead to implementing inadequate or inappropriate security controls.

Although FMS and the Federal Reserve had documented and implemented many security controls to protect Pay.gov, security controls were not always effectively implemented to ensure the confidentiality, integrity, and availability of the Pay.gov environment and data. FMS and the Federal Reserve established and documented key security and control policies and procedures for Pay.gov. In addition, they established numerous controls intended to restrict access to the application and computing environment and performed several security reviews to identify and mitigate vulnerabilities. However, numerous information security control weaknesses increased the risk that external and internal users could gain unauthorized access to Pay.gov, which could lead to the inappropriate disclosure or modification of its data or to the disruption of service. For example,

- FMS and the Federal Reserve had not consistently implemented access controls to prevent, limit, and detect electronic access to the Pay.gov application and computing environment. These weaknesses involved user accounts and passwords, access rights and permissions, and network services and security, as well as auditing and monitoring security-relevant events.

- In addition, weaknesses in other information systems controls—such as segregation of duties, software change controls, service continuity, and application security controls—reduced FMS's effectiveness in mitigating the risk of errors or fraud, preventing unauthorized changes to software, and ensuring the continuity of data processing operations when unexpected interruptions occur.

These computer weaknesses existed, in part, because FMS did not provide sufficient management oversight of Pay.gov operating personnel at the Federal Reserve facilities to ensure that elements of the Pay.gov computer security program were fully or consistently implemented.

# Contents



**Abbreviations**

| | |
|---|---|
| FMS | Financial Management Service |
| NIST | National Institute of Standards and Technology |
| OMB | Office of Management and Budget |
| TWAI | Treasury Web Application Infrastructure |

GAO
Accountability * Integrity * Reliability

**United States General Accounting Office**
**Washington, D.C. 20548**

July 30, 2003

The Honorable Tom Davis
Chairman
Committee on Government Reform
House of Representatives

The Honorable Adam H. Putnam
Chairman
Subcommittee on Technology, Information Policy,
Intergovernmental Relations, and the Census
Committee on Government Reform
House of Representatives

The federal government is moving toward implementing Web-based electronic government to provide public services. At the same time, the computer systems that support these services face increasing security risks from viruses, hackers, and others who seek to interrupt federal operations or to obtain sensitive information that is stored in federal computers.

One of the more significant federal electronic government initiatives, "Pay.gov," is an Internet portal and transaction engine created and managed by the Department of the Treasury's Financial Management Service (FMS) and operated, maintained, and tested at three Federal Reserve facilities. Pay.gov allows the public to make certain non-income-tax-related payments to the federal government via the Internet. Still early in its implementation, Pay.gov is estimated to eventually handle up to 80 million transactions valued at $125 billion annually.

Because the magnitude of transaction volume and dollar value envisioned for Pay.gov could result in substantial harm to the federal government if the site were successfully attacked, the former chairman of the expired Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, Committee on Government Reform, requested that we review this initiative. He asked us to determine whether the agency (1) conducted a comprehensive security risk assessment and (2) documented and implemented appropriate security measures and controls for the system's protection.

To accomplish this, we interviewed FMS officials and examined Pay.gov risk assessment documents to determine the procedures used to assess risks. We also observed and tested the effectiveness of information security

controls in operation for the Pay.gov application and the computing environment in which it operates. We are addressing this report to you in response to your request.

We are also issuing to you a version of this report that provides a more detailed discussion of the information security weaknesses affecting Pay.gov and additional technical recommendations. Because some of the weaknesses are sensitive and could jeopardize FMS's ability to protect Pay.gov if released to the public, that report is designated "Limited Official Use Only."

## Results in Brief

FMS had not fully assessed the risks associated with the Pay.gov initiative. Although FMS prepared a business risk assessment for the application, it had not assessed the risks associated with the Pay.gov computing environment because officials incorrectly believed such an assessment was not necessary. Insufficient assessment of risks can lead to the implementation of inadequate or inappropriate security controls.

Although FMS and the Federal Reserve have documented and implemented many security controls to protect Pay.gov, security controls and practices have not always been effectively implemented to ensure the confidentiality, integrity, and availability of the Pay.gov computing environment and data. FMS and the Federal Reserve have established and documented key security policies and procedures for Pay.gov. In addition, they have established numerous controls intended to restrict access to the application and computing environment and performed several security reviews to identify and mitigate vulnerabilities. Yet, numerous information security control weaknesses increased the risk that external and internal users could have gained unauthorized access to Pay.gov, which could have led to the inappropriate disclosure or modification of its data or to the disruption of service. For example, FMS and the Federal Reserve had not consistently implemented access controls to prevent, limit, and detect electronic access to the application and computing environment. In addition, weaknesses in other information system controls (segregation of duties, software change controls, and service continuity) and application security controls reduced FMS's effectiveness in mitigating the risk of errors or fraud, preventing unauthorized changes to software, and ensuring the continuity of data processing operations when unexpected interruptions occur.

These computer control weaknesses existed, in part, because FMS did not provide sufficient management oversight to ensure that Pay.gov operating personnel at Federal Reserve facilities fully or consistently implemented elements of the Pay.gov information security program. We are making recommendations that address these weaknesses. FMS has asserted that it took immediate action to correct most of the weaknesses we identified and has plans to correct those that remain. In providing written comments on a draft of this report, the FMS Commissioner concurred with our recommendations, identified specific corrective actions that FMS has taken to address the recommendations, and provided other comments.

## 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 the public's trust is essential. The dramatic expansion in computer interconnectivity and the rapid increase in the use of the Internet are changing the way our government, the nation, and much of the world communicate and conduct business. Without proper safeguards, such interconnectivity also poses enormous risks that make it easier for individuals and groups with malicious intent to intrude into inadequately protected systems and use such access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks.

Protecting the computer systems that support critical operations and infrastructures has never been more important because of concerns about attacks from individuals and groups with such malicious intent, including terrorists. These concerns are well founded for a number of reasons, including the dramatic increases in reported computer 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 cyber attacks to come.

Computer-supported federal operations are likewise at risk. Our previous reports, and those of agency inspectors general, describe persistent computer security weaknesses that place a variety of critical federal operations, including those at FMS, at risk of disruption, fraud, and inappropriate disclosure.[1] This body of audit evidence led us, in 1997, to designate computer security as a governmentwide high-risk area in reports to the Congress.[2] It remains so today.[3]

How well federal agencies are addressing these risks is a topic of increasing interest in both the Congress and the executive branch. This is evidenced by recent hearings on information security[4] and recent legislation intended to strengthen information security.[5] In addition, the administration has taken other important actions to improve information security, such as integrating information security into the President's Management Agenda Scorecard. Moreover, the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) have issued security guidance to agencies.

[1]U.S. General Accounting Office, *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies*, GAO/AIMD-00-295 (Washington, D.C.: Sept. 6, 2000).

[2]U.S. General Accounting Office, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: February 1997).

[3]U.S. General Accounting Office, *High-Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures*, GAO-03-121 (Washington, D.C.: January 2003).

[4]U.S. General Accounting Office, *Information Security: Progress Made, But Challenges Remain to Effectively Protect Federal Systems and the Nation's Critical Infrastructures*, GAO-03-564T (Washington, D.C.: Apr. 8, 2003); *Computer Security: Progress Made, But Critical Federal Operations and Assets Remain at Risk*, GAO-03-303T (Washington, D.C.: Nov. 19, 2002); *Information Security: Comments on the Proposed Federal Information Security Management Act of 2002*, GAO-02-677T (Washington, D.C.: May 2, 2002); and *Information Security: Additional Actions Needed to Implement Reform Legislation*, GAO-02-470T (Washington, D.C.: Mar. 6, 2002).

[5]E-Government Act of 2002 (P.L. 107-347, Title III, Section 301, Dec. 17, 2002) and Government Information Security Provisions in the Fiscal Year 2001 Defense Authorization Act (P. L. 106-398, Division A, Title X, Subtitle G, Section 1061, Oct. 30, 2000).

## FMS is the Federal Government's Financial Manager

FMS is the bureau of the U.S. Department of the Treasury that serves as the federal government's financial manager. Its mission is to provide central payment services to federal agencies, operate federal collection and deposit systems, manage delinquent debt owed to the federal government, and provide governmentwide accounting and reporting services. FMS processes about $3 trillion in collections and disbursements annually.

To help it accomplish its mission, FMS maintains multiple financial and information systems to help it process and reconcile monies disbursed and collected by the various government agencies. These banking, collection, and disbursement systems are also used to process agency transactions, record relevant data, transfer funds to and from the Treasury, and facilitate the reconciliation of those transactions. In addition to its own data processing centers, FMS relies on contractors and the Federal Reserve to help carry out its financial management services.

## Pay.gov is a Key Electronic Government Initiative

FMS's Pay.gov is a governmentwide transaction portal that allows federal agencies to collect and the public to make several types of payments to the federal government via the Internet. Citizens and businesses remitting funds to the government for fees, fines, sales, leases, loan repayments, donations, and certain taxes[6] can authorize Pay.gov to process an automated clearing house debit against their bank account or to authorize and settle a credit card transaction. In addition to collections, Pay.gov is to provide other electronic financial services over the Internet to assist federal agencies, such as (1) presenting agency bills to end users for collection and (2) accepting agency forms submitted by end users. Pay.gov is also to provide access control service that verifies an end user's identity (authentication) and authorizes the end user's allowed actions. Its reporting service provides information to the Treasury, agencies, and the public about transactions.

Pay.gov is to support program needs of agencies and cash flow management for the Department of the Treasury. Critical information assets of this system include information provided by end users for authentication as well as form, bill, and collection data that are housed in Pay.gov's databases and provided to the relevant agencies.

[6]These include excise taxes, but do not include income tax payments. Income tax payments are handled through separate systems.

According to FMS, the benefits of using Pay.gov include (1) increasing user convenience because electronic forms can be filed at any time, including outside of normal business hours, and (2) helping agencies meet their requirements under the Government Paperwork Elimination Act, which requires federal agencies to accept certain forms electronically by October 2003, when practicable as a substitute for paper.

Although still early in its implementation, Pay.gov transaction volumes and amounts are expected to be significant. FMS has estimated that Pay.gov eventually could process about 80 million transactions and collect about $125 billion a year. According to FMS, during fiscal year 2002, Pay.gov collected about $1.5 billion in direct debit transactions.[7] As of October 2002, Pay.gov was processing 20,000 direct debit transactions a month.

Pay.gov is part of the Treasury Web Application Infrastructure (TWAI), a new Treasury hosting environment operated by the Federal Reserve. According to the Federal Reserve, TWAI is completely separate from its own payment systems and computing infrastructure. TWAI, referred to as the Pay.gov computing environment in this report, is designed to host multiple Treasury applications, of which Pay.gov is only one. It comprises a production or operating environment at one Federal Reserve facility and a test environment for testing and quality assurance services at another. In addition, a second production or operating environment is planned for the Pay.gov computing environment at a third Federal Reserve facility.

The Assistant Commissioner, Federal Finance, is responsible for the federal government's collection and deposit systems, including Pay.gov. A dedicated program manager oversees and manages the Pay.gov initiative for FMS. Responsibility for implementing and maintaining information technology security requirements for Pay.gov and its computing environment has been delegated to two information system security officers. Under the direction of FMS, several Federal Reserve facilities and their contractors operate Pay.gov and its computing environment and perform hosting, collection, and customer service functions.

[7]Direct debit transactions are electronic funds transfers processed through the Automated Clearing House network.

## Objectives, Scope, and Methodology

The objectives of our review were to determine whether FMS (1) conducted a comprehensive security risk assessment for Pay.gov and (2) documented and implemented appropriate security measures and controls for the system's protection.

To determine if a risk assessment was conducted for Pay.gov, we requested and examined risk assessment documents prepared for the Pay.gov application and computing environment. We also interviewed agency officials and reviewed risk assessment procedures.

To guide our work for assessing Pay.gov security controls, we used the audit methodology described in our *Federal Information System Controls Audit Manual*, which discusses the scope of such reviews and the type of testing required for evaluating controls intended to

- limit, detect, and monitor electronic access to computer resources (data, programs, equipment, and facilities), thereby protecting these resources against unauthorized disclosure, modification, and use;
- ensure that work responsibilities are segregated so that one individual does not perform or control key aspects of computer-related operations and thereby have the ability to conduct unauthorized actions or gain unauthorized access to assets or records;
- prevent the implementation of unauthorized programs or modifications to an existing program; and
- minimize the risk of unplanned interruptions and recover critical computer processing operations if interruptions occur.

To evaluate these controls, we reviewed system documentation, policies, and procedures; tested and observed controls in operation for the Pay.gov application and its computing environment located at three Federal Reserve facilities; and examined reports and other documents regarding security design and implementation. We also discussed with key security representatives, system administrators, and management officials whether computer-related controls were in place, adequately designed, and operating effectively.

We performed our review at the Financial Management Service in Washington, D.C., three Federal Reserve facilities, and at our headquarters

in Washington, D.C., from October 2002 through June 2003, in accordance with generally accepted government auditing standards.

## Pay.gov Risks Were Not Fully Assessed

Understanding the risks associated with information systems is a key element of an information security program. Identifying and assessing information security risks help to determine what controls are required and what level of resources should be expended on controls. The Federal Information Security Management Act of 2002 and its predecessor, the Government Information Security Reform provisions,[8] require all federal agencies to develop comprehensive information security programs based on assessing and managing risks. The February 1996 revision to OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, directs agencies to use a risk-based approach to determine adequate security, including a consideration of the major factors in risk management: the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards.

FMS assessed certain risks associated with the Pay.gov initiative; however, some key risks, including those relevant to the Pay.gov computing environment, were not sufficiently considered. FMS prepared a business risk assessment for the Pay.gov application in June 2002, about 9 months after Pay.gov's initial release but just prior to the migration of the application from a private-sector service provider to the Federal Reserve. The assessment identified Pay.gov critical assets and the possible threats and vulnerabilities to those assets. Pay.gov stakeholders then assessed those threats, their associated vulnerabilities, and the consequences of the threats in order to prioritize and assign a risk level (for example, high, medium, or low) for each threat. Next, FMS identified and analyzed the existing controls and residual risks and then devised a plan of action to mitigate the risks to the Pay.gov application.

[8]During the period when we performed our audit work, the two major laws related to federal computer information security in effect were the Computer Security Act, Public Law 100-235, January 8, 1988, and the Government Information Security Reform provisions (GISRA), Title X, Subtitle G, Public Law 106-398, October 30, 2000. Effective December 17, 2002, the Federal Information Security Management Act of 2002, Title III, Public Law 107-347, repealed GISRA and the Computer Security Act, and replaced them with similar, but strengthened, provisions.

However, FMS did not sufficiently assess the risk associated with the Pay.gov computing environment. This environment, which FMS defined as a general support system, provides the infrastructure for Treasury's Web-based applications, including Pay.gov. FMS continued to host applications such as Pay.gov in this computing environment without taking necessary steps to identify and address potential threats to the system. For example, FMS had not conducted a business risk assessment for the computing environment because officials did not believe this was necessary. Although FMS's process for certification and accreditation[9] required a business risk assessment for the Pay.gov application, it did not require one for the computing environment. By not fully assessing risks, FMS is more likely to implement inadequate or inappropriate security controls that do not address the system's true risks, which can lead to costly efforts to subsequently implement effective controls.

## Although Many Controls Were Established, Weaknesses Posed Risks to Pay.gov

The effective implementation of appropriate, properly designed security controls is an essential element for ensuring the confidentiality, integrity, and availability of computerized systems and data. Weak security controls expose computerized systems and data to an increased risk of disclosure, modification, and use.

Although FMS and the Federal Reserve established many policies, procedures, and controls to protect Pay.gov resources, they did not always effectively implement security controls and practices to ensure the confidentiality, integrity, and availability of Pay.gov's computing environment and data. Weaknesses in electronic access controls placed data at risk of unauthorized access, which could lead to their unauthorized disclosure, modification, and use. In addition, weaknesses in other information system controls, including segregation of duties, software change controls, service continuity, and application security controls, further increased risk to Pay.gov.

[9]Certification is an evaluation process resulting in a judgment stating whether or not an information system meets a prespecified set of security requirements. Accreditation is an official management authorization for an information system to process data in an operational environment at an acceptable level of residual risk.

## FMS and the Federal Reserve Had Established Many Controls for Pay.gov

Prior to our review, FMS and the Federal Reserve had taken action to protect Pay.gov and its computing environment. It established key security and control policies and procedures in various system documents, including system security plans, security concept of operations, contingency plans, and configuration management plans. For example, the *TWAI System Security Plan* presents an overview of the security requirements of the system and describes the controls in place or planned for meeting those requirements. This document also delineates responsibilities and expected behavior of all individuals who access the system.

FMS and the Federal Reserve implemented numerous controls intended to restrict access to Pay.gov and its computing environment. These controls included (1) designing a layered, multizone security architecture to restrict user access to sensitive components; (2) installing multiple sets of firewalls from three different vendors to control external and internal access across the computing environment; (3) deploying a network intrusion detection capability to monitor network activity; (4) establishing controls to confirm the identity of users and to limit access to authorized levels; (5) implementing encrypted protocols to manage devices; (6) disallowing direct inbound Internet connectivity to the internal network; (7) prohibiting incoming E-mail; (8) using a more secure network protocol for file sharing; and (9) employing a team of competent system administrators. Further, FMS performed several security reviews to identify and mitigate vulnerabilities associated with Pay.gov. The implementation of these controls helped to provide a "defense-in-depth" approach to securing Pay.gov resources.

FMS and the Federal Reserve had also established other information system controls designed to protect the integrity and availability of the Pay.gov computing environment. Both the development and production teams involved in Pay.gov activities had instituted several software change management policies and procedures that helped to ensure that only authorized programs and modifications were implemented. For example, change control boards for Pay.gov and its computing production environment effectively conducted review and authorization of proposed software changes and determined whether or not to include the changes in the software release. FMS also hired independent reviewers to conduct technical and software process assessments, resulting in the establishment of improved procedures in the Pay.gov software development process. Procedures used to make emergency changes in the production Pay.gov computing environment were appropriate. Moreover, the development and

production teams maintained an effective record-keeping system of software change requests, thereby providing sufficient audit trails of their activities. FMS and the Federal Reserve had also implemented local redundancy of hardware, software, and telecommunications in the Pay.gov production computing environment to reduce the risk of service interruption.

Despite these controls, numerous information security control weaknesses increased the risk that external and internal users could have gained unauthorized access to Pay.gov, which could have led to the inappropriate disclosure or modification of its data or to the disruption of service.

## Electronic Access Controls Were Not Consistently Implemented

A basic management objective for any organization is the protection of its information systems and critical data from unauthorized access. Organizations accomplish this objective by designing and implementing controls that are designed to prevent, limit, and detect electronic access to computing resources. These controls include user accounts and passwords, access permissions and rights, network services and security, and audit and monitoring of security-relevant events. Inadequate logical access controls diminish the reliability of computerized data and increase the risk of unauthorized access, which could lead to unauthorized disclosure, modification, and use of data.

FMS and the Federal Reserve did not consistently implement effective electronic access controls to prevent, limit, and detect access to Pay.gov and its computing environment. Numerous vulnerabilities existed in Pay.gov's computing environment because of the cumulative effects of control weaknesses in the areas of user accounts and passwords, access permissions and rights, network services and security, and audit and monitoring of security-related events. For example, outdated software versions existed that were exploitable from the Internet and could have provided an attacker with root access to a server in the Pay.gov computing environment. From the vulnerable server, an attacker would have had direct access to the management network that interconnected and bypassed the firewalls for each of the security zones. By doing so, an attacker could have exploited other vulnerabilities, such as test accounts and easily guessed passwords, vulnerable services, and insecurely configured X Windows servers. Also, because of weaknesses in real-time alerting and the lack of an intrusion detection system on an internal network, the likelihood of detection would have been remote. Weaknesses in the specific control areas are summarized below.

## User Accounts and Passwords

A computer system must be able to identify and differentiate among users so that activities on the system can be linked to specific individuals. Unique user accounts assigned to specific users allow systems to distinguish one user from another, a process called identification. The system must also establish the validity of a user's claimed identity through some means of authentication, such as a secret password, 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 controlling access to the system. Accordingly, agencies should (1) implement procedures to control the creation, use, and removal of user accounts and (2) establish password parameters, such as length, life, and composition, to strengthen the effectiveness of account/password combinations for authenticating the identity of users.

FMS and the Federal Reserve did not sufficiently control user accounts and passwords to ensure that only authorized individuals were granted access to the systems and data. For example, Pay.gov operating personnel did not consistently configure password parameters securely, and users sometimes created easy-to-guess passwords. A commonly known vendor-supplied password was not removed from one server, and passwords on another were inappropriately stored in clear text, increasing the likelihood of their disclosure and unauthorized use to gain access to server resources. Moreover, users were not required to enter a unique user ID to log on to certain network devices, thereby diminishing FMS's ability to attribute system activity to the responsible individual. These practices increase the risk that individuals might gain unauthorized access to Pay.gov resources without attribution.

## Access Rights and Permissions

A basic underlying principle for securing computer systems and data is the concept of least privilege. This means that users are granted only those access rights and permissions needed to perform their official duties. Organizations establish access rights and permissions to restrict the access of legitimate users to the specific programs and files that they need to do their work. User rights are allowable actions that can be assigned to users or groups. File and directory permissions are rules associated with a file or directory that regulate which users can access them and in what manner. Assignment of rights and permissions must be carefully considered to avoid giving users unintentional and unnecessary access to sensitive files and directories.

FMS and the Federal Reserve routinely permitted excessive access to the Pay.gov computing environment and to certain key files and directories.

For example, Pay.gov operating personnel permitted numerous world-writable or world-readable files[10] on servers. In addition, operating personnel did not sufficiently configure the content of users' profiles on certain servers in the Pay.gov computing environment, increasing the risk that malicious software could be introduced on the servers. Inappropriate access to sensitive utilities, system directories, and other sensitive files, as well as overly permissive inbound access rules, provides opportunities for individuals to circumvent security controls to read, modify, or delete critical or sensitive information and programs.

## Network Services and Security

Networks are series of interconnected devices and software that allow individuals to share data and computer programs. Because sensitive programs and data are stored on or transmitted along networks, effectively securing networks is essential to protecting computing resources and data from unauthorized access, manipulation, and use. Organizations secure their networks, in part, by installing and configuring network devices that permit authorized network service requests and deny unauthorized requests and by limiting the services that are available on the network. Network devices include (1) firewalls designed to prevent unauthorized access into the network, (2) routers that filter and forward data along the network, (3) switches that forward information among parts of a network, and (4) servers that host applications and data. Network services consist of protocols for transmitting data between computers. Insecurely configured network services and devices can make a system vulnerable to internal or external threats, such as denial-of-service attacks.[11] Since networks often provide the entry point for access to electronic information assets, failure to secure them increases the risk of unauthorized use of sensitive data and systems.

FMS and the Federal Reserve enabled vulnerable, outdated, and/or misconfigured network services and devices. For example, Pay.gov operating personnel used outdated versions of system software and configured network devices to permit vulnerable services. They also did not sufficiently restrict incoming traffic on a number of firewalls or effectively restrict access to or from a management network in the Pay.gov

[10]World-writable or world-readable permissions allow all system users to modify or view the contents of the file.

[11]A denial-of-service attack is an attack on a network that prevents legitimate use of the network.

computing environment. Running vulnerable network services and insecurely configuring network devices increase the risk of system compromise, such as unauthorized access to and manipulation of sensitive system data, disruption of services, and denial of service.

### Audit and Monitoring of Security-Relevant Events

Determining what, when, and by whom specific actions were taken on a system is crucial to establishing individual accountability, monitoring compliance with security policies, and investigating security violations. 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 monitoring users' activities. How organizations configure the system or security software determines the nature and extent of audit trail information that is provided. To be effective, organizations should (1) configure the software to collect and maintain sufficient audit trail information[12] for security-relevant events;[13] (2) generate reports that selectively identify unauthorized, unusual, and sensitive access activity; and (3) regularly monitor and take action on these reports. Without sufficient auditing and monitoring, organizations increase the risk that they may not detect unauthorized activities or policy violations.

FMS and the Federal Reserve did not consistently monitor system activity on firewalls and servers in the Pay.gov computing environment. For example, logging was inconsistently implemented on firewalls, and there was no capability to monitor system activity as it occurred. In addition, FMS did not fully implement a network intrusion detection capability. As a result, increased risk exists that unauthorized access to the servers and data may not be detected in a timely manner.

## Other Information System Controls Need Improvement

In addition to electronic access controls, other important controls should be in place to ensure the confidentiality, integrity, and availability of an information system's software programs and data. These information system controls include policies, procedures, and techniques that properly

[12]Audit trail information generally includes the (1) date and time the event occurred, (2) user ID associated with the event, (3) type of event, and (4) result of the event.

[13]Security-relevant events include (1) successful and unsuccessful log-on attempts; (2) log-offs; (3) change of password; (4) creation, deletion, opening, and closing of files; (5) all actions of users with privileged authority; and (6) program initiation.

segregate incompatible duties among computer personnel, appropriately prevent unauthorized software changes, and effectively ensure the continuation of operations in case of unexpected interruption. Weaknesses in these areas increase the risk of unauthorized access, disclosure, and modification of the system's programs and data.

## Segregation of Duties

Segregation of duties refers to the policies, procedures, and organizational structure that help ensure that one individual cannot independently control all key aspects of a process or computer-related operation and thereby conduct unauthorized actions or gain unauthorized access to assets or records. Often, segregation of duties is achieved by dividing responsibilities among two or more organizational groups. Dividing duties among two or more individuals or groups diminishes the likelihood that errors and wrongful acts will go undetected because the activities of one individual or group will serve as a check on the activities of the other. Inadequate segregation of duties increases the risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, and computer resources damaged or destroyed.

FMS and the Federal Reserve did not consistently separate certain incompatible functions among Pay.gov operating personnel. For example, they did not sufficiently separate incompatible system administration and security administration duties of Pay.gov operating personnel at a Federal Reserve facility. To illustrate, the same individuals were responsible for adding and deleting systems users and for maintaining system audit logs. This condition existed, in part, because FMS lacked implementing guidelines for separating incompatible duties among personnel administering the Pay.gov computing environment. As a consequence, increased risk exists that these individuals could perform unauthorized system activities without being detected.

## Software Change Controls

Also important for an organization's information security is ensuring that only authorized application programs are placed in operation. This is accomplished by instituting policies, procedures, and techniques that help ensure that all programs and program modifications are properly authorized, tested, and approved. Moreover, access to programs should be restricted to authorized personnel only. Failure to do so increases the risk that unauthorized programs or changes could be inadvertently or deliberately placed into operation.

Weaknesses in software change control procedures threatened the integrity and reliability of the Pay.gov application and data. For example, FMS and

the Federal Reserve established change control procedures that provided developers with access to Pay.gov software source code after the code had been tested and approved for operation. This provided an opportunity for the developer to inadvertently or deliberately make unauthorized changes to the source code before it was placed into operation and consequently corrupt data. In addition, key information was not consistently provided on software change request forms, thereby increasing the risk that changes could be inappropriately implemented. Furthermore, the Pay.gov's software change management procedures lacked the inclusion of certain standards for prioritizing, scheduling, and testing software changes, which could potentially lead to inconsistent or arbitrary decisions regarding software changes.

### Service Continuity

Service continuity controls should be designed to ensure that when unexpected events occur, key operations continue without interruption or are promptly resumed, and critical and sensitive data are protected. These controls include environmental controls and procedures designed to protect information resources and minimize the risk of unplanned interruptions, along with a well-tested plan to recover critical operations should interruptions occur. If service continuity controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete financial or management information.

Service continuity controls for Pay.gov were not mature. For example, contingency plans for the Pay.gov application and computing environment did not identify key personnel, did not contain detailed procedures to restore operations, and had not been tested. In addition, back-up tapes were not stored at an off-site facility. Further, all Windows servers in the hosting environment did not have antivirus software installed. As a result, FMS has diminished assurance that it will be able to promptly recover essential Pay.gov processing operations if an unexpected interruption occurs.

## Pay.gov Application Control Weaknesses Introduce Risk

Application security controls help ensure that unauthorized individuals cannot gain access and that authorized users can only enter legitimate transactions or perform appropriate system activities.

The Federal Reserve implemented effective procedures for establishing user accounts on the Pay.gov application and distributing initial passwords to users. However, the application was designed with weak password

controls and inadequate audit logging and reporting of security-relevant events. As a result, increased risk exists that unauthorized individuals and authorized users can gain access to Pay.gov application and enter erroneous transactions or conduct inappropriate system activities without detection.

## FMS Did Not Provide Sufficient Management Oversight for Pay.gov

These weaknesses existed, in part, because FMS did not provide sufficient management oversight of Pay.gov operating personnel to ensure that key elements of an information security program for Pay.gov and its computing environment were fully or consistently implemented. Although the Federal Reserve and its contractor operate and maintain the Pay.gov computing environment and application, FMS, as the program manager, is responsible for managing, securing, and overseeing the operation of Pay.gov. Our prior study of strong security management practices[14] found that leading organizations handle their information security risks through an ongoing cycle of risk management. This process includes (1) assessing risks and determining what security measures are needed, (2) establishing and implementing policies and controls that meet those needs, (3) promoting security awareness so that users understand the risks and the related policies and controls in place to mitigate those risks, and (4) monitoring policies and controls to ensure they are appropriate and effective and that known weaknesses are promptly mitigated. Although FMS and the Federal Reserve had implemented numerous controls for Pay.gov, the security of Pay.gov systems and data was diminished because FMS did not ensure that risks were fully assessed, policies and controls were effectively implemented, operating personnel were aware of strong security practices, known weaknesses were promptly mitigated, and systems were reviewed for security exposures after changes to the systems were made.

- As previously discussed, FMS did not sufficiently assess risks for the Pay.gov computing environment because it did not require a business risk assessment for certification and accreditation and officials did not believe one was necessary. By not fully assessing risks, FMS was more likely to implement inadequate or inappropriate security controls that do not address the environment's true risks, which could lead to costly efforts to subsequently implement effective controls.

[14]U.S. General Accounting Office, *Information Security Management: Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

- Another key element of an effective information security program is establishing and implementing appropriate policies and related controls. FMS established information security policies for Pay.gov in documents such as the security concept of operations, system security plans, and security policy that, in general, reflect strong security practices. However, FMS and Pay.gov operating personnel did not consistently implement them. Many weaknesses identified in this report existed because FMS or Pay.gov operating personnel at Federal Reserve facilities did not comply with security policies. A key factor for this is that FMS had not sufficiently documented specific standards or detailed guidelines for implementing those policies. For example, about 49 percent of the weaknesses identified in this report existed, in part, because FMS had not developed or provided guidelines in sufficient detail for implementing controls or configuring systems. The documentation of standards and guidelines is important because it provides system administrators and other operating personnel specific instructions on how to, among other things, implement controls and configure systems in order to comply with agency information security policies.

- Another important element of an information security program involves promoting awareness and providing required training so that users understand the risks and their role in implementing related policies and controls to mitigate those risks. However, the extent of noncompliance with strong security policies and guidelines suggests that some operating personnel were either unaware of appropriate security practices or insensitive to the need for implementing important information system controls.

- An ongoing monitoring program that includes testing and evaluation helps to ensure that systems are in compliance with policies, and that policies and controls are both appropriate and effective. This type of oversight is fundamental because it demonstrates management's commitment to the security program, reminds employees of their roles and responsibilities, and identifies and mitigates areas of noncompliance and ineffectiveness. Although contractors conducted several reviews of controls for the Pay.gov computing environment, Pay.gov operating personnel did not consistently or promptly correct identified weaknesses. For example, about 22 percent of the weaknesses we identified during our review had been identified in these prior reviews, including a serious vulnerability related to the security zones established for the Pay.gov computing environment.

- In particular, a key component of an ongoing monitoring process is the review of security configuration settings on devices after software has been installed or maintenance has been performed. Operating personnel are often required to change security configuration settings on systems in order to install new software or devices and to perform maintenance on existing ones. Because of this change, it is important to ensure that these security settings are reset to their secure values when the installation or maintenance is completed. However, FMS did not ensure that operating personnel performed a postinstallation review to identify vulnerable configuration settings after a new release of Pay.gov was installed. Operating personnel stated that some of the weaknesses we identified could have occurred when system security settings were changed to install the new release but not reset to their secure value after the installation was complete.

These deficiencies are consistent with those we previously reported on FMS oversight of its other contractors that provide operational support for key FMS financial systems.[15]

## FMS Asserts It Has Corrected Many Weaknesses

FMS generally agreed with the weaknesses we identified and took immediate steps to address them. FMS asserted that half of the weaknesses had been addressed during or within 1 week following our on-site review and that it has since corrected 47 of the 49 weaknesses identified. FMS is actively working to address the remaining two weaknesses. Prompt implementation of these actions by FMS demonstrates a commitment to securing Pay.gov resources.

# Conclusions

Although FMS and the Federal Reserve had implemented numerous controls to protect Pay.gov computing resources, risks were not sufficiently assessed, and numerous control weaknesses increased risks to the confidentiality, integrity, and availability of Pay.gov systems and data because FMS did not provide sufficient management oversight to ensure that key elements of the Pay.gov information security program were fully or consistently implemented. While FMS has asserted that it has taken immediate action to correct the weaknesses that we identified during our

[15]U.S. General Accounting Office, *Financial Management Service: Significant Weaknesses in Computer Controls Continue*, GAO-02-317 (Washington, D.C.: Jan. 31, 2002).

review, much work remains to be done to enable FMS and the Federal Reserve to promptly address new security threats and risks as they emerge. Ensuring that known weaknesses affecting the Pay.gov application and its computing environment are promptly mitigated requires top management support and leadership, disciplined processes, and consistent oversight. Until FMS ensures that steps are completed to mitigate these weaknesses and address emerging ones, it will have reduced assurance that the Pay.gov application and computing environment are safeguarded against misuse and unauthorized disclosure and modification, and its exposure to these risks will remain unnecessarily high.

## Recommendations for Executive Action

To ensure the confidentiality, integrity, and availability of the Pay.gov application and computing environment, we recommend that the FMS Commissioner direct the Pay.gov program manager to develop and implement an action plan for strengthening Pay.gov computer controls.

In addition, we recommend that FMS Commissioner strengthen management oversight of the Pay.gov initiative by directing the Pay.gov program manager to

- assess risks for the Pay.gov computing environment,
- develop technical implementation guidance to (1) assist Pay.gov operating personnel with implementing controls and configuring Pay.gov devices in accordance with strong security practice and (2) document reasons for using less secure configuration settings,
- track and actively coordinate with Pay.gov operating personnel to correct or mitigate known weaknesses and report the status of corrective actions to the FMS Commissioner on a regular basis, and
- establish procedures for the proactive review or audit of the configuration settings on Pay.gov devices after installation or maintenance.

## Agency Comments

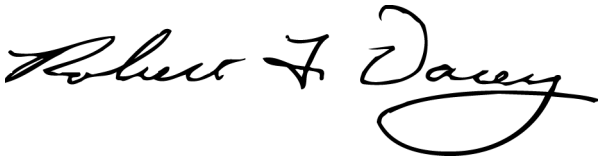
In providing written comments on a draft of this report (which are reprinted in app. I), the FMS Commissioner concurred with our recommendations and noted that FMS had already implemented 96 percent of the recommendations in the Limited Official Use Only version of this

report, with the rest to be addressed as part of an upcoming release of Pay.gov. The Commissioner also identified the specific corrective actions that FMS has taken to strengthen management oversight of the Pay.gov initiative. These include (1) completing a comprehensive security risk assessment for the Pay.gov computing environment; (2) documenting and implementing appropriate security and management controls to protect the application and its computing environment; (3) establishing a team to periodically check the configuration of servers and networks, as well as to evaluate operational staff awareness of and adherence to established policy; (4) engaging the Federal Reserve's National Incident Response Team and establishing an agreement with the Federal Reserve that the general auditors of the various Reserve Banks will conduct regular information technology audits of FMS's Internet applications; (5) instituting greater separation of duties and a more rigorous software change management process to maintain stricter control over deployed software; and (6) documenting security policies in all statements of work so that all vendors are aware of and accountable for security requirements. According to the FMS Commissioner, these actions have already helped to more consistently enforce security controls over Pay.gov.

The FMS Commissioner takes issue with one element of our assessment. Throughout this report, we attribute many of the weaknesses jointly to FMS and the Federal Reserve. The Commissioner believes it is inappropriate and unnecessary to include the Federal Reserve as a responsible party to the report's findings because all management responsibility and authority over all business, technical, and policy decisions reside exclusively with FMS. We agree with the FMS Commissioner that management responsibility rests with FMS, which is why we have addressed our recommendations to the Commissioner. However, we also believe it is appropriate and necessary to include the Federal Reserve as a responsible party because (1) the Pay.gov application and computing environment reside at Federal Reserve facilities, (2) the Federal Reserve's personnel and contractors are responsible for operating the Pay.gov application and computing environment, and (3) day-to-day operational decisions and activities by the Federal Reserve's personnel or contractors contributed to the security weaknesses affecting Pay.gov.

If you have any questions or need any further information, please contact Gregory C. Wilshusen, Assistant Director, at (202) 512-6244, or me at (202) 512-3317. We can also be reached by E-mail at wilshuseng@gao.gov or

daceyr@gao.gov, respectively. Key contributors to this report are identified in app. II.



Robert F. Dacey
Director, Information Security Issues

# Comments from the Financial Management Service

COMMISSIONER

DEPARTMENT OF THE TREASURY
FINANCIAL MANAGEMENT SERVICE
WASHINGTON, D.C. 20227

July 18, 2003

Mr. Robert F. Dacey
Director, Information Security Issues
United States General Accounting Office
Washington, D.C. 20548

Dear Mr. Dacey:

Thank you for the opportunity to comment on the July 2003 draft audit report entitled "INFORMATION SECURITY: Computer Controls over Key Treasury Internet Payment System" (GAO-03-837). We concur with the General Accounting Office's (GAO) recommendations in the report. The Financial Management Service (FMS) believes that this GAO assessment has resulted in an improved security posture for Pay.gov as well as for the Treasury Web Application Infrastructure (TWAI), the computing environment in which Pay.gov operates.

FMS appreciates GAO's recognition of the sound designs and practices we have employed on Pay.gov and the TWAI. We also are cognizant of the fact that GAO has acknowledged our responsiveness in addressing the findings in the report. We continually give considerable thought to architectural principles, comprehensive security policy, and security practices in order to deploy robust systems.

It is important to note that at the time this report was delivered, FMS had already implemented 96% of recommendations in the report. The rest will be addressed as part of the upcoming 3.0 release of Pay.gov, which is scheduled for implementation in Spring 2004.

FMS has taken the following specific corrective actions:

- We have completed a comprehensive security risk assessment for the Pay.gov computing environment (the TWAI).[1] The "Treasury Web Application Infrastructure Business Risk Assessment" has been available for review since November 4, 2002.

- We have documented and implemented appropriate security and management controls to protect the application and its computing environment. We have codified operational procedures to ensure that our servers and networks maintain proper configurations from the time a device is introduced into the computing environment and throughout its life cycle.

[1] The review of technical controls was done in compliance with NIST 800-26 and 800-30.

Page 2 – Mr. Robert F. Dacey

- We have established a TWAI Information Security Team to periodically check the configuration of servers and networks, as well as to evaluate operational staff awareness of and adherence to established policy. We have also engaged the Federal Reserve's National Incident Response Team, and have established an agreement with the Federal Reserve that the general auditors of the various Reserve Banks will conduct regular information technology audits of our Internet applications.

- We have instituted greater separation of duties and a more rigorous software change management process to maintain stricter control over the deployed code.

- TWAI security policies are now documented in all statements of work, regardless of the work activity, so that all vendors are aware of and accountable for security requirements whenever a change is made to the computing environment.

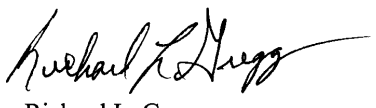
FMS believes that these steps address the underlying causes of the GAO findings, the vast majority of which resulted from the introduction of new hardware into the computing environment. These actions have already helped to more consistently enforce our security controls.

FMS respectfully takes issue with one element of the GAO assessment. Throughout the main body of the report, GAO attributes failures and weaknesses to FMS and the Federal Reserve jointly. The Federal Reserve's role in support of Pay.gov is to serve as FMS' fiscal agent and to provide services at our direction. All management responsibility and authority over all business, technical, and policy decisions, however, have always resided exclusively with FMS. We believe it is inappropriate and unnecessary to include the Federal Reserve as a responsible party to the report's findings.

In summary, FMS has documented and implemented new security policies and procedures, and we have worked hard to ensure that all operating personnel comply with these. We have also established new roles and engaged additional support staff for periodic tests, security reviews, audits, and additional separation of duties.

Thank you for the opportunity to respond.

Sincerely,



Richard L. Gregg

cc: Donald V. Hammond
Louise Roseman

# GAO Contact and Staff Acknowledgments

## GAO Contact

Gregory C. Wilshusen, Assistant Director (202) 512-6244

## Staff Acknowledgments

In addition to the individual named above, Lon Chin, West Coile, Debbi Conner, Kristi Dorsey, Kenneth Johnson, Hal Lewis, Duc Ngo, Thomas Payne, Henry Sutanto, and Christopher Warweg made key contributions to this report.

## GAO's Mission

The General Accounting 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 the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

## 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. General Accounting 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

## Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

**United States**
**General Accounting Office**
**Washington, D.C. 20548-0001**

**Official Business**
**Penalty for Private Use $300**

**Address Service Requested**

**Presorted Standard**
**Postage & Fees Paid**
**GAO**
**Permit No. GI00**