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.