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.