January 2009

INFORMATION SECURITY

Further Actions Needed to Address Risks to Bank Secrecy Act Data

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-09-195, a report to congressional requesters

Why GAO Did This Study

The Financial Crimes Enforcement Network (FinCEN), a bureau within the Department of the Treasury, relies extensively on its own computer systems, as well as those at the Internal Revenue Service (IRS) and the Treasury Communications System (TCS), to administer the Bank Secrecy Act (BSA) and fulfill its mission of safeguarding the U.S. financial system from financial crimes. Effective information security controls over these systems are essential to ensuring that BSA data, which contains sensitive financial information used by law enforcement agencies to prosecute financial crime, is protected from inappropriate or deliberate misuse, improper disclosure, or destruction.

GAO evaluated whether security controls that effectively protect the confidentiality, integrity, and availability of the information and systems that support FinCEN's mission have been implemented. To do this, GAO examined security policies and controls for systems at three organizations.

What GAO Recommends

GAO recommends that the Secretary of the Treasury direct the FinCEN Director to take several actions to fully implement an effective agencywide information security program. In commenting on a draft of this report, Treasury agreed to develop a detailed corrective action plan for each of the recommendations.

To view the full product, including the scope and methodology, click on GAO-09-195. For more information, contact Nancy Kingsbury at (202) 512-2700 or kingsburyn@gao.gov, or Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

FinCEN, TCS, and IRS have taken important steps in implementing numerous controls to protect the information and systems that support FinCEN's mission; however, significant information security weaknesses remain in protecting the confidentiality, integrity, and availability of these systems and information. The three organizations implemented many information security controls to protect the information and systems that support FinCEN's mission. For example, IRS controlled changes to a key application and FinCEN segregated areas of its network. Nonetheless, the organizations had inconsistently applied or not fully implemented controls to prevent, limit, or detect unauthorized access to this information and these systems. For example, the organizations did not always (1) implement user and password management controls for properly identifying and authenticating users, (2) restrict user access to data to only what was required for performing job functions, (3) adequately encrypt data, (4) protect the external and internal boundaries on its systems, and (5) log user activity on databases. Furthermore, weaknesses in which systems were insecurely configured and patches were not applied to critical systems also existed. As a result, sensitive information used by the federal government, financial institutions, and law enforcement agencies to combat money laundering and terrorist financing is at an increased risk of unauthorized use, modification, or disclosure.

A key reason for many of the weaknesses was that FinCEN and IRS had not fully implemented key information security program activities. For example, FinCEN did not always include detailed implementation guidance in its policies and procedures and adequately test and evaluate information security controls. Furthermore, GAO has previously reported that IRS did not sufficiently verify whether remedial actions were implemented or effective in mitigating vulnerabilities and recommended that it implement a revised remedial action verification process.