April 2007

INFORMATION SECURITY

FBI Needs to Address Weaknesses in Critical Network

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-368, a report to F. James Sensenbrenner Jr., House of Representatives

Why GAO Did This Study

The Federal Bureau of Investigation (FBI) relies on a critical network to electronically communicate, capture, exchange, and access law enforcement and investigative information. Misuse or interruption of this critical network, or disclosure of the information traversing it, would impair FBI's ability to fulfill its missions. Effective information security controls are essential for ensuring that information technology resources and information are adequately protected from inadvertent or deliberate misuse, fraudulent use, disclosure, modification, or destruction.

GAO was asked to assess information security controls for one of FBI's critical networks. To assess controls, GAO conducted a vulnerability assessment of the internal network and evaluated the bureau's information security program associated with the network operating environment. This report summarizes weaknesses in information security controls in one of FBI's critical networks.

What GAO Recommends

GAO recommends several actions to fully implement an information security program. In a separate classified report, GAO makes recommendations to correct specific weaknesses. FBI agreed with many of the recommendations but disagreed with the characterization of risk to its information and noted that it has made significant strides in reducing risks. GAO believes that increased risk remains.

www.gao.gov/cgi-bin/getrpt?GAO-07-368.

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

Certain information security controls over the critical internal network reviewed were ineffective in protecting the confidentiality, integrity, and availability of information and information resources. Specifically, FBI did not consistently (1) configure network devices and services to prevent unauthorized insider access and ensure system integrity; (2) identify and authenticate users to prevent unauthorized access; (3) enforce the principle of least privilege to ensure that authorized access was necessary and appropriate; (4) apply strong encryption techniques to protect sensitive data on its networks; (5) log, audit, or monitor security-related events; (6) protect the physical security of its network; and (7) patch key servers and workstations in a timely manner. Taken collectively, these weaknesses place sensitive information transmitted on the network at risk of unauthorized disclosure or modification, and could result in a disruption of service, increasing the bureau's vulnerability to insider threats.

These weaknesses existed, in part, because FBI had not fully implemented key information security program activities for the critical network reviewed. FBI has developed an agencywide information security program, which includes an organization to monitor and protect the bureau's information systems from external attacks and insider misuse and to serve as the central focal point of contact for near-real-time security monitoring. However, shortcomings exist with certain program elements for the network, including an outdated risk assessment, incomplete security plan, incomplete specialized security training, insufficient testing, untimely remediation of weaknesses, and inadequate service continuity planning. Without a fully implemented program, certain security controls will likely remain inadequate or inconsistently applied.