October 2010

INFORMATION SECURITY

National Archives and Records Administration Needs to Implement Key Program Elements and Controls

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-11-20, a report to the Ranking Member, Committee on Finance, U.S. Senate

Why GAO Did This Study

The National Archives and Records Administration (NARA) is responsible for preserving access to government documents and other records of historical significance and overseeing records management throughout the federal government. NARA relies on the use of information systems to receive, process, store, and track government records. As such, NARA is tasked with preserving and maintaining access to increasing volumes of electronic records.

GAO was asked to determine whether NARA has effectively implemented appropriate information security controls to protect the confidentiality, integrity, and availability of the information and systems that support its mission. To do this, GAO tested security controls over NARA's key networks and systems; reviewed policies, plans, and reports; and interviewed officials at nine sites.

What GAO Recommends

GAO is making 11 recommendations to the Archivist of the United States to implement elements of NARA's information security program. In commenting on a draft of this report, the Archivist generally concurred with GAO's recommendations but disagreed with some of the report's findings. GAO continues to believe that the findings are valid.

View GAO-11-20 or key components. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov and Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

What GAO Found

NARA has not effectively implemented information security controls to sufficiently protect the confidentiality, integrity, and availability of the information and systems that support its mission. Although it has developed a policy for granting or denying access rights to its resources, employed mechanisms to prevent and respond to security breaches, and made use of encryption technologies to protect sensitive data, significant weaknesses pervade its systems. NARA did not fully implement access controls, which are designed to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities. Specifically, the agency did not always (1) protect the boundaries of its networks by, for example, ensuring that all incoming traffic was inspected by a firewall; (2) enforce strong policies for identifying and authenticating users by, for example, requiring the use of complex (i.e., not easily guessed) passwords; (3) limit users' access to systems to what was required for them to perform their official duties; (4) ensure that sensitive information, such as passwords for system administration, was encrypted so as not to be easily readable by potentially malicious individuals; (5) keep logs of network activity or monitor all parts of its networks for possible security incidents; and (6) implement physical controls on access to its systems and information, such as securing perimeter and exterior doors and controlling visitor access to computing facilities.

In addition to weaknesses in access controls, NARA had mixed results in implementing other security controls. For example:

- NARA did not always ensure equipment used for sanitization (i.e., wiping clean of data) and disposal of media (e.g., hard drives) was tested to verify correct performance.
- NARA conducted appropriate background investigations for employees and contractors to ensure sufficient clearance requirements have been met before permitting access to information and information systems.
- NARA did not consistently segregate duties among various personnel to ensure that no one person or group can independently control all key aspects of a process or operation.

The identified weaknesses can be attributed to NARA not fully implementing key elements of its information security program. Specifically, the agency did not adequately assess risks facing its systems, consistently prepare and document security plans for its information systems, effectively ensure that all personnel were given relevant security training, effectively test systems' security controls, consistently track security incidents, and develop contingency plans for all its systems. Collectively, these weaknesses could place sensitive information, such as records containing personally identifiable information, at increased and unnecessary risk of unauthorized access, disclosure, modification, or loss.