GAO
Accountability * Integrity * Reliability
Highlights

Highlights of GAO-13-63, a report to congressional requesters

January 2013

INFORMATION SECURITY

Actions Needed by Census Bureau to Address Weaknesses

Why GAO Did This Study

The Census Bureau is responsible for collecting and providing data about the people and economy of the United States. The bureau has long used some form of automation to tabulate the data it collects. Critical to the bureau's ability to perform these duties are its information systems and the protection of the information they contain. A data breach could result in the public's loss of confidence in the bureau's and could affect its ability to collect census data.

Because of the importance of protecting information and systems at the bureau, GAO was asked to determine whether the agency 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 the bureau's key networks and systems; reviewed policies, plans, and reports; and interviewed officials at bureau headquarters and field offices.

What GAO Recommends

GAO is making 13 recommendations to the Census Bureau to enhance its agencywide information security program and, in a separate report with limited distribution, making an additional 102 recommendations. In written comments, the Department of Commerce expressed broad agreement with the overall theme of the report and said it would work to identify the best way to address our recommendations, but did not directly comment on the recommendations. It raised concerns about specific aspects of the reported findings which GAO addressed as appropriate.

View GAO-13-63. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

What GAO Found

Although the Census Bureau has taken steps to safeguard the information and systems that support its mission, it has not effectively implemented appropriate information security controls to protect those systems. Many of the deficiencies relate to the security controls used to regulate who or what can access the bureau's systems (access controls). For example, the bureau did not adequately: control connectivity to key network devices and servers; identify and authenticate users; limit user access rights and permissions to only those necessary to perform official duties; encrypt data in transmission and at rest; monitor its systems and network; or ensure appropriate physical security controls were in place. Without adequate controls over access to its systems, the bureau cannot be sure that its information and systems are protected from intrusion.

In addition to access controls, implementing other important security controls including policies, procedures, and techniques to implement system configurations and plan for and manage unplanned events (contingency planning) helps to ensure the confidentiality, integrity, and availability of information and systems. While the Census Bureau had documented policies and procedures for managing and implementing configuration management controls, key communication systems were not securely configured and did not have proper encryption. Further, while the bureau has taken steps to implement guidance for contingency planning such as developing plans for mitigating disruptions to its primary data center through the use of emergency power, fire suppression, and storing backup copies of data for its critical systems offsite at a secured location, it only partially satisfied other requirements for contingency planning such as distributing the plan to key personnel and identifying potential weaknesses during disaster testing. Without an effective and complete contingency plan, an agency's likelihood of recovering its information and systems in a timely manner is diminished.

An underlying reason for these weaknesses is that the Census Bureau has not fully implemented a comprehensive information security program to ensure that controls are effectively established and maintained. Specifically, the Census Bureau had begun implementing a new risk management framework with a goal of better management visibility of information security risks, but the framework did not fully document identified information security risks. Also, the bureau had not updated certain security management program policies, adequately enforced user requirements for security and awareness training, and implemented policies and procedures for incident response. Until the bureau implements a complete and comprehensive security program, it will have limited assurance that its information and systems are being adequately protected against unauthorized access, use, disclosure, modification, disruption, or loss.