United States Government Accountability Office

GAO

Report to Congressional Requesters

January 2013

INFORMATION SECURITY

Actions Needed by Census Bureau to Address Weaknesses

GAO
Accountability * Integrity * Reliability

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.

Contents

Tables

Figures

Abbreviations

CCTV	closed circuit television
CD-ROM	compact disc/read-only memory
Census Bureau	U.S. Census Bureau
DHS	Department of Homeland Security
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
IT	information technology
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OMB	Office of Management and Budget
PIV	personal identity verification
US-CERT	United States Computer Emergency Readiness Team

G A O
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

January 22, 2013

The Honorable Thomas R. Carper
United States Senate

The Honorable Danny K. Davis
U.S. House of Representatives

Providing current and relevant data about the economy and people of the United States is the mission of the Department of Commerce's Census Bureau. The data collected are vital for reapportionment and redistricting decisions for seats of the House of Representatives; realigning the boundaries of the legislative districts of each state; allocating money for federal financial assistance; and providing a social, demographic, and economic profile of the nation's people to guide policy decisions at each level of government. To improve the coverage, accuracy, and efficiency of gathering data from the public, the Census Bureau relies on automation and technology. In turn, the public relies on the bureau to keep its personal information secure. A data breach could result in the public's loss of confidence in the bureau's ability to secure personal information and could affect the bureau's ability to carry out its mission.

Given the Census Bureau's extensive use of information technology (IT) in collecting, analyzing, and distributing information, and the importance of keeping the information it gathers secure, you asked us to determine the extent to which the bureau has effectively implemented appropriate information security controls to protect the confidentiality, integrity, and availability of the information and systems that support its mission.

To address our objective, we examined information security controls over the Census Bureau's network infrastructure and systems key to its mission. We also examined bureau information security policies, plans, and procedures; reviewed the bureau's testing of controls over key systems; interviewed agency officials; and reviewed Department of Commerce Inspector General reports to identify previously-reported weaknesses. For more information on our objective, scope, and methodology, see appendix I.

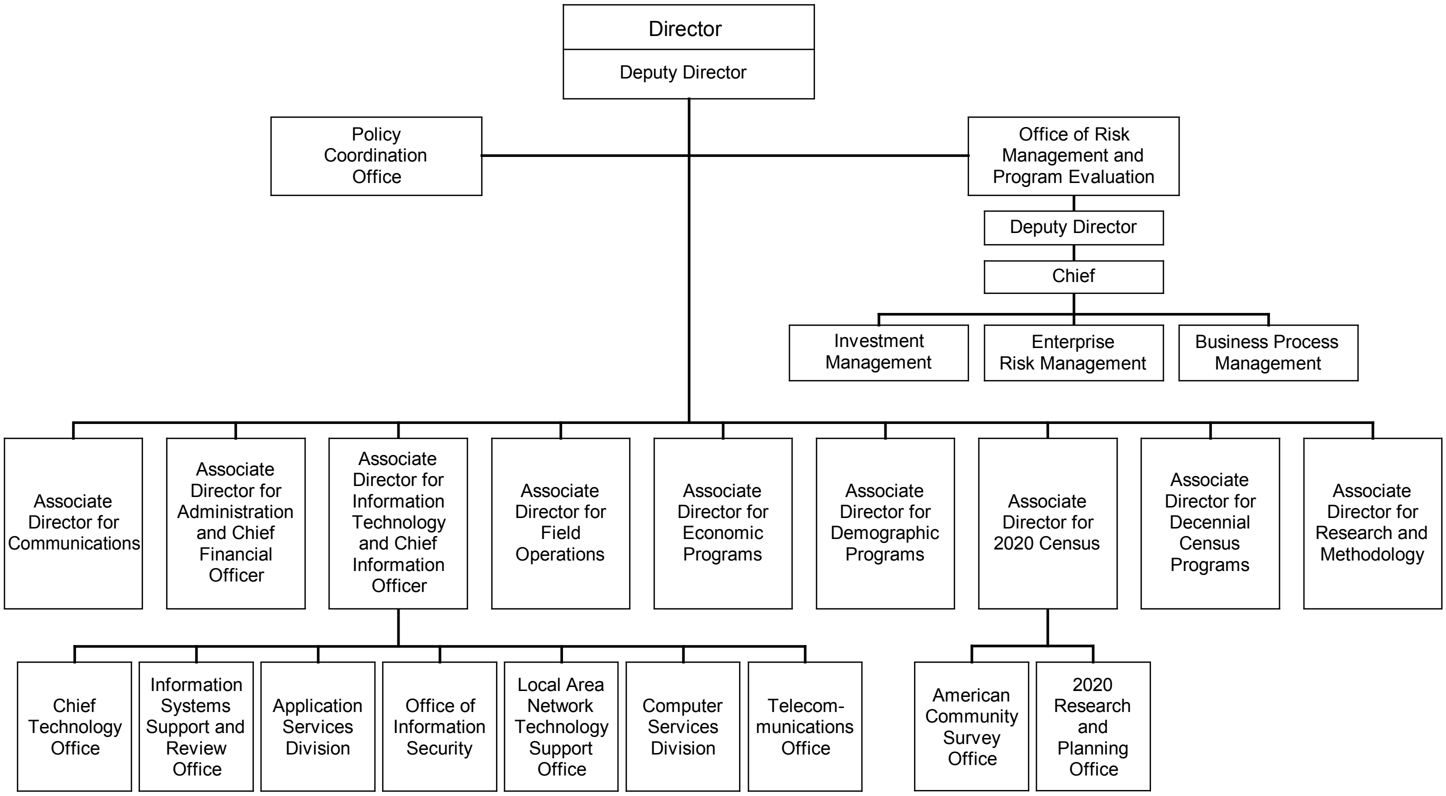
We conducted this performance audit from January 2012 through January 2013 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The Census Bureau's mission is to collect and provide comprehensive data about the nation's people and economy. Core activities include conducting decennial, economic, and government censuses; conducting demographic and economic surveys; managing international demographic and socioeconomic databases; providing technical advisory services to foreign governments; and performing other activities such as producing official population estimates and projections.

The Census Bureau is part of the Department of Commerce and is in the department's Economics and Statistics Administration, led by the Under Secretary for Economic Affairs. It is headed by a director and is organized into directorates corresponding to key programmatic and administrative functions, as depicted in figure 1.

Figure 1: Organization of the Census Bureau



Director
Deputy Director
Policy Coordination Office
Office of Risk Management and Program Evaluation
Deputy Director
Chief
Investment Management
Enterprise Risk Management
Business Process Management
Associate Director for Communications
Associate Director for Administration and Chief Financial Officer
Associate Director for Information Technology and Chief Information Officer
Associate Director for Field Operations
Associate Director for Economic Programs
Associate Director for Demographic Programs
Associate Director for 2020 Census
Associate Director for Decennial Census Programs
Associate Director for Research and Methodology
Chief Technology Office
Information Systems Support and Review Office
Application Services Division
Office of Information Security
Local Area Network Technology Support Office
Computer Services Division
Telecom-munications Office
American Community Survey Office
2020 Research and Planning Office

Source: GAO analysis of Census Bureau documents.

To support the IT operations for all of its activities, including those related to decennial censuses, the Census Bureau reported that it planned to spend $384 million on major IT investments in fiscal year 2012.

Role of IT at the Census Bureau

The Census Bureau's mission to plan, take, process, and publish the results of censuses and surveys requires the work of thousands of people and, increasingly, the use of automation to compile the information. For nearly 100 years, census data were tabulated by clerks who made tally marks or added columns of figures with a pen or a pencil. As the nation grew and there were more people, items, and characteristics to count, speedier tabulation methods had to be invented or the results of one census would not be processed before it was time for the next one. In 1880, the bureau used a "tabulating machine"—a wooden box in which a roll of paper was threaded past an opening where a clerk marked the tallies in various columns and then added up the marks when the roll was full—which made tabulating at least twice as fast as the previously-used manual processes.

By 1950, mechanical tabulating improved to 2,000 items per minute. In 1951, the bureau used the first large-scale electronic computer, UNIVAC I, designed and built specifically for its use. This machine was able to tabulate 4,000 items per minute. Beginning in 1970, the bureau took advantage of new high-speed equipment that converted data on computer tape directly to words and numbers on off-set negative film used in publishing. Then, in the mid-1980s, statistics were made available on diskettes for use in microcomputers and users were able to obtain statistics online. In the later 1980s, the bureau began testing CD-ROM (compact disc/read-only memory) laser disks as a medium for releasing data.

The 2000 census demonstrated probably the biggest leap forward in the use of technology for collecting and disseminating data. The bureau's previous response scanning system (which dated to the 1950s) was replaced with optical character recognition technology, allowing the bureau to design a respondent-friendly (instead of machine-friendly) questionnaire in which write-in responses could also be captured electronically. In addition, the bureau's previous online data system from the 1990s evolved into online data available through the Census Bureau's website.[1] Further technological advances were made in the 2010 Decennial Census through the use of handheld computers for parts of census operations and the integration of Global Positioning System information into Census Bureau maps.

While advances in capturing and tabulating census data can improve the bureau's ability to fulfill its mission, the costs for these improvements have been high. The 2010 Decennial Census, at $13 billion, was the most expensive U.S. census in history. One reason for this was the greater-than-anticipated use of paper-based processing due to performance issues with key IT systems, which increased the price of the census by almost $3 billion. Based on these past trends, the cost of the next

[1] See http://www.census.gov.

decennial census could reach approximately $25 billion,[2] although, thus far, the bureau is planning to spend roughly $12 to $18 billion.

Title 13 Protects Sensitive Census Bureau Information

For many years, each decennial census was conducted pursuant to a specific act of Congress. In 1954, that body of acts was brought together in Title 13 of the United States Code,[3] the laws under which the Census Bureau operates. Title 13 spells out the basic scope of the censuses and surveys, the requirements for the public to provide information as well as for the Census Bureau to keep that information confidential, and the penalties for violating these obligations. Specifically, the bureau may not disclose or publish any private information that identifies an individual or business, such as names, addresses, Social Security numbers, and telephone numbers. Other federal laws, including the Confidential Information Protection and Statistical Efficiency Act of 2002[4] and the Privacy Act of 1974,[5] reinforce these protections.

According to bureau documentation, the bureau takes several steps to protect the public's personal information. For example, it displays its data protection and privacy principles on its website,[6] pledges to remove personally identifiable information—such as names, telephone numbers, and addresses—from data files, and uses various approaches to protect personal information, including computer technologies, statistical methodologies, and security procedures. For example, according to the bureau, names and addresses are removed from forms, the remaining information is transferred to a machine readable form, and the original questionnaires are then destroyed. Before any census tabulation is published, it is checked to make certain that no individual, household, or organization can be identified, and that information cannot be inferred by

[2] GAO has issued several reports on challenges with and lessons learned from the 2010 Decennial Census. See, for example, GAO, *2010 Census: Preliminary Lessons Learned Highlight the Need for Fundamental Reforms*, GAO-11-496T (Washington, D.C.: Apr. 6, 2011).

[3] 13 U.S.C. §§ 1 - 402.

[4] 44 U.S.C. § 3501 note.

[5] 5 U.S.C. § 552a.

[6] The web page is part of the Bureau of the Census' main website. This page was accessed 10/23/2012: http://www.census.gov/privacy/data_protection/our_privacy_principles.html.

reading the table or by analyzing the figures it contains. Every person who works with the bureau's confidential information takes an oath to uphold the law. Violating the confidentiality of a respondent is a federal crime with serious penalties, including a federal prison sentence of up to 5 years, a fine of up to $250,000, or both.

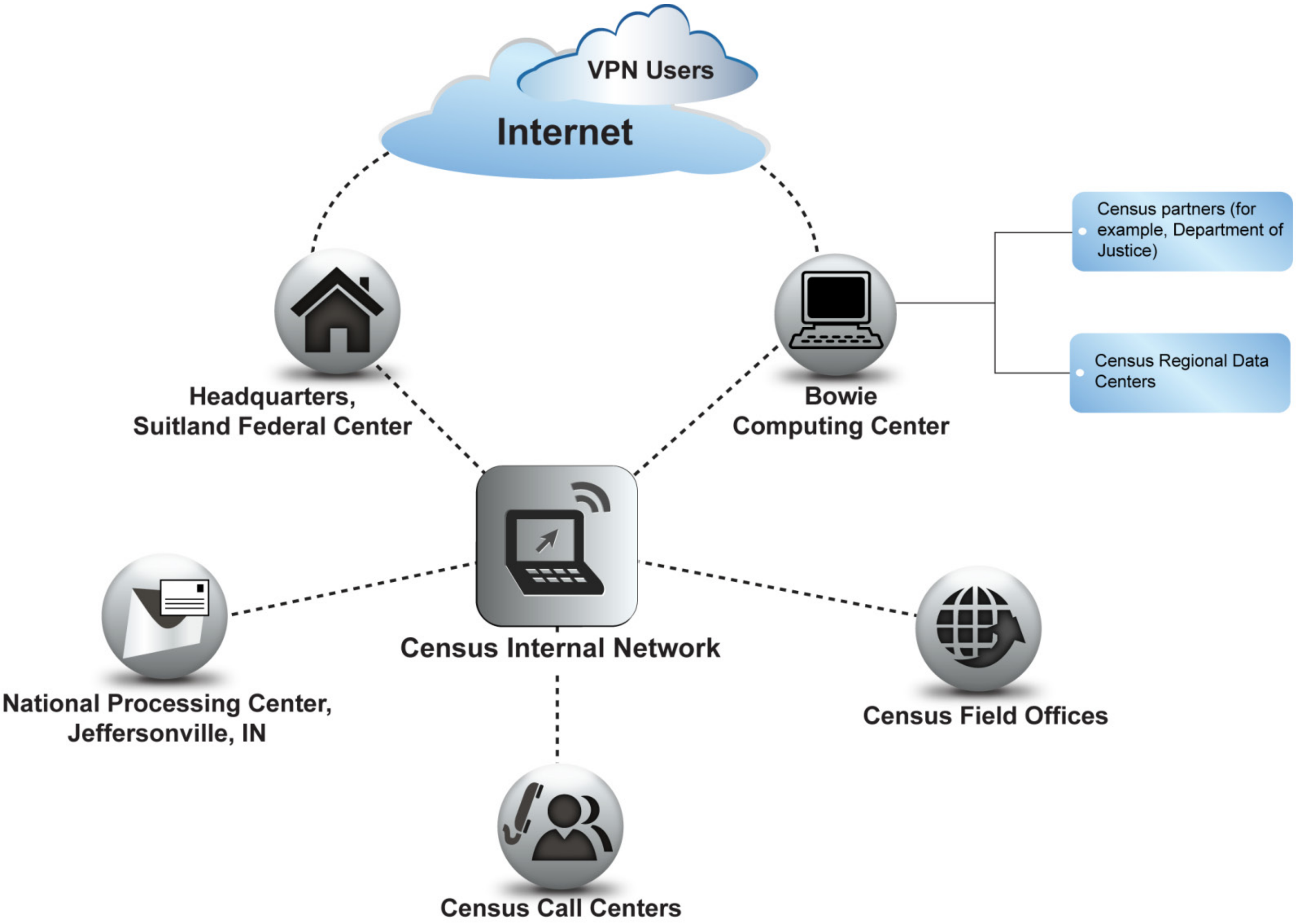
According to the Census Bureau, results from previous censuses are stored in secure locations. In the case of population and housing census data, the questionnaires are microfilmed before destruction and the microfilm is stored in the bureau's National Processing Center in Jeffersonville, Indiana, where an individual or an heir or legal representative may obtain information for proof of age or residence in the form of an official transcript. Copies of population census schedules from 1790 through 1940, are available for research at the National Archives, on the Internet, and at libraries in various parts of the country, but subsequent records are closed to the public for 72 years to protect the confidentiality of the information they contain. (The Freedom of Information Act, designed to make records available to individuals, does not apply to identifiable data the Census Bureau collects for statistical purposes.)[7]

[7] 5 U.S.C. § 552(b)(3); 13 U.S.C. § 9.

Responsibility for Census Bureau Information Systems

The bureau's IT operations are divided among three locations: Census Bureau headquarters in Suitland, Maryland; the Bowie Computing Center in Bowie, Maryland; and the National Processing Center in Jeffersonville, Indiana. See figure 2 for a depiction of the Census Bureau's network.

Figure 2: Simplified Depiction of Census Bureau Network


VPN Users
Internet
Census partners (for example, Department of Justice)
Census Regional Data Centers
Headquarters, Suitland Federal Center
Bowie Computing Center
Census Internal Network
National Processing Center, Jeffersonville, IN
Census Field Offices
Census Call Centers

Source: GAO Analysis of Census Bureau documentation and interviews.

At these locations, the Census Bureau's information systems are organized into 27 "CENs," with each CEN containing a set of information resources that share the same direct management control. These systems include networks, telecommunications, and specific applications.

Headquarters develops national policies and is the primary location hosting the bureau's statistical programs. The Bowie Computing Center is the bureau's primary data center, and the National Processing Center is the bureau's primary location for mailing, receiving, and scanning data from hard copy survey forms. The bureau has additional facilities nationwide, including field offices, regional data centers, and call centers.

Many of the bureau's enterprise IT resources and services are managed by the Information Technology Directorate, which is led by the Associate Director for Information Technology, who serves as the Chief Information Officer for the bureau. Within the IT Directorate, three offices play key roles in administering Census Bureau IT operations: (1) the Telecommunications Office, at headquarters in Suitland, is responsible for operating the wide area network that provides connectivity among headquarters, major sites, regional offices, and other government agencies; (2) the Local Area Network Technologies Support Office, also located in Suitland, manages end user desktops, core productivity applications, and connectivity from user workstations to the core network; and (3) the Computer Services Division, located in Bowie, manages server operations across the bureau.

Responsibility for other key IT systems lies within other bureau organizations, and the majority of the bureau's IT staff are located outside of the bureau's IT Directorate. According to the Census Bureau, of 1,148 IT staff,[8] the IT Directorate has 256, Economic Programs has 262, the Decennial Census has 156, Field Operations has 185, and Demographic Programs has 123. In addition, according to the bureau, the IT Directorate was allocated $130 million in fiscal year 2012 to be spent on systems it manages and $254 million was allocated for systems managed by other directorates.

[8] As reported in July 2012 by a bureau official from the Human Resources Division.

FISMA Establishes Responsibilities for the Census Bureau's Information Security Program

The Federal Information Security Management Act of 2002 (FISMA)[9] requires each federal agency to develop, document, and implement an agencywide information security program to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by other agencies, contractors, or other sources. The Secretary of Commerce is responsible for ensuring that the department, including the Census Bureau, provides an information security program, commensurate with risk, for information collected or maintained by or on behalf of the agency, and information systems used or operated by the agency or on its behalf. The Secretary, as agency head is also responsible for ensuring that senior agency officials, such as the Under Secretary for Economic Affairs who oversees the Census Bureau, provide information security for the operations and assets under their control.

The Director of the Census Bureau is accountable to the Department of Commerce for the Census Bureau's information security program, and has delegated oversight of the program to the bureau's Chief Information Officer. The Census Bureau's Chief Information Officer has appointed the bureau's Chief Information Security Officer to serve as the bureau's Senior Agency Information Security Officer. The Chief Information Security Officer is responsible for ensuring that the bureau's information security program follows applicable federal laws.

The Office of Information Security, led by the bureau's Chief Information Security Officer, centrally administers the bureau's information security program. The bureau has designated key roles in IT security according to FISMA and the bureau's IT security policies (see table 1).

[9] FISMA was enacted as title III of the E-Government Act of 2002, Pub. L. No.107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). FISMA requires each federal agency to report to specified congressional committees, GAO, and the Director of OMB each year on agency compliance with the act's information security requirements. The Census Bureau reports on FISMA compliance through its parent agency, the Department of Commerce.

Table 1: Positions with Key Information Security Responsibilities at the Census Bureau

Position	Key responsibilities
Chief Information Officer	Manages the IT security program, and develops, maintains and oversees the IT security policy. Ensures that the IT security program complies with FISMA. Serves as the authorizing official or co-authorizing official, as necessary, for systems within the operating unit.
Chief Information Security Officer	Serves as the bureau’s Chief Information Security Officer. Leads the Census Bureau’s Office of Information Security. Develops and maintains IT security policy, procedures, standards, and guidance. Ensures effective implementation of and compliance with established policies and procedures. Participates in the IT security community and briefs senior bureau officials on incidents and potential threats.
Authorizing Official	Has the authority to assume responsibility for funding and operating an information system at an acceptable level of risk to operations, assets, and individuals. Authorizes security requirements, system security plans, interconnection system agreements, and memoranda of understanding. For systems related to a particular directorate, the Associate Director and CIO serve as co-authorizing officials. For IT infrastructure systems, the Chief Information Officer serves as the sole authorizing official.
Information System Owner	Responsible for the overall procurement, development, integration, modification, and operation and maintenance of an information system. This includes determining who has access to the system, and with what rights and privileges. Generally located in the directorate that the information system supports.
Information Security Manager	Serves as the principal security risk advisor, provides oversight functions, and coordinates and disseminates information security matters on behalf of a directorate. There is generally a separate information security manager for each directorate.
Information System Security Officer	Located within an individual directorate, serves as the principal advisor to the Office of Information Security, and security officer on all security matters for an information system. In coordination with the security officer, the Information System Security Officer develops and updates the system security plan, manages and controls changes to the system, and assesses the security impact of those changes.
Information Owner	Responsible for establishing the rules for appropriate use and protection of information, including controls on generation, collection, processing, dissemination, and disposal.
IT Security Incident Response Personnel	Located within the bureau’s Office of Information Security, analyze and work to reduce cyber threats and vulnerabilities, disseminate cyber threat warning information, and coordinate incident response activities with Department of Commerce computer incident response teams and the United States Computer Emergency Readiness Team.
Certification Agent	Located within the bureau’s Office of Information Security. The individual, group, or organization responsible for conducting a security certification, or comprehensive assessment of the security controls in an information system, to determine the extent to which the controls are implemented correctly and are meeting the security requirements for the system. The certification agent also recommends corrective actions to reduce or eliminate vulnerabilities in the information system.

Source: GAO analysis of Census Bureau documentation.

Control Weaknesses Threaten Information and Systems that Support Census Bureau Mission

Although the Census Bureau has taken steps to safeguard the information and systems that support its mission, security control weaknesses pervaded its systems and networks, thereby jeopardizing the bureau's ability to sufficiently protect the confidentiality, integrity, and availability of its information and systems. These deficiencies included those related to access controls, as well as other controls such as configuration management and contingency planning. A key reason for these weaknesses is that the bureau has not yet fully implemented an agencywide information security program to ensure that controls are appropriately designed and operating effectively. As a result, the bureau has limited assurance that its information and information systems are being adequately protected against unauthorized access, use, disclosure, modification, disruption, or loss.

Census Bureau Did Not Fully Implement Access Controls

Access controls are designed and implemented to ensure the reliability of an agency's computerized information. Both logical and physical access controls are intended to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities. Access controls include those related to (1) protection of system boundaries, (2) identification and authentication, (3) authorization, (4) cryptography, (5) audit and monitoring, and (6) physical security. Inadequate design or implementation of access controls increases the risk of unauthorized disclosure, modification, and destruction of sensitive information and disruption of service.

Boundaries for Network Devices Not Sufficiently Controlled

Boundary protection controls logical connectivity into and out of networks and controls connectivity to and from devices connected to the network. For example, multiple firewalls can be deployed to prevent both outsiders and trusted insiders from gaining unauthorized access to systems, and intrusion detection technologies can be deployed to defend against attacks from the Internet. Unnecessary connectivity to an organization's network increases not only the number of access paths that must be managed and the complexity of the task, but also the risk of unauthorized access in a shared environment. NIST guidance states that agencies should provide adequate protection for networks and employ information control policies and enforcement mechanisms to control the flow of information between designated sources and destinations within information systems.[10] The National Security Agency (NSA) provides leading practices that agencies may adopt for securing and configuring information systems. These practices include establishing a dedicated management network, also called an out-of-band network, to provide several benefits, such as allowing parallel management of all devices, fault analysis, and recovery and recommend against the use of unencrypted protocols to manage IT infrastructure.

The Census Bureau had taken steps to protect network boundaries. For example, the bureau used firewalls to protect its network from unwanted Internet intrusions. The bureau had also implemented an intrusion detection system[11] on key network segments to monitor for malicious network activity.

However, the bureau did not sufficiently control connectivity to key network devices and servers. Specifically, the bureau did not protect access to its network devices and servers by using a separate dedicated network for centralized management and administration of many network devices and servers. Rather, various bureau management activities were on the general network and therefore were more vulnerable to compromise because of the broader access to the general network. In the event that the bureau's general network is compromised, there is an increased risk that the bureau may not be able to manage its systems or even detect an attack. In addition, the bureau was using insecure protocols to manage its IT infrastructure, placing sensitive data such as administrative user accounts and passwords at risk of compromise.

Systems and Network Protocols Did Not Appropriately Enforce Authentication for Users

A computer system must be able to identify and authenticate different users so that activities on the system can be linked to a specific individual. When an organization assigns a unique user account to a specific user, the system is able to distinguish that user from another—a process called identification. The system must also establish the validity of a user's claimed identity by requesting some kind of information, such as a password, that is known only by the user—a process known as

[10] NIST, *Recommended Security Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 3 (Gaithersburg, Md., August 2009).

[11] An intrusion detection system is a hardware or software product that gathers and analyzes information from various areas within a computer or network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

authentication. The combination of identification and authentication—such as a user account/password combination—provides the basis for establishing individual accountability and for controlling access to the system. NIST 800-53 guidelines recommend that information systems uniquely identify and authenticate all users (or processes on behalf of users) and that systems be set to establish complex passwords to reduce the likelihood of a successful attack. Census Bureau policy also requires minimum standards for password parameters such as complexity, minimum and maximum lifetime restrictions, reuse, and account lock out.

Furthermore, Office of Management and Budget (OMB) guidelines direct federal agencies to use multifactor authentication for remote access to agency systems[12] and NIST guidelines recommend that when using cryptographic keys for authentication, the authentication process prove possession and control of the encryption key. Typically, this requires that the key be encrypted using some form of activation data such as a password. Additionally, bureau policy states that encryption keys should be changed periodically. NIST guidelines also recommend that, before devices establish a connection, they should be identified and authenticated.

Finally, in February 2011, OMB directed agencies to issue implementation policies for personal identity verification cards (PIV), used to verify employee identity, by March 31, 2011.[13] Agencies were required to use PIV credentials as the common means of authentication for physical and logical access to agency facilities, networks, and information systems. A PIV card must contain the personally identifiable information for the employee or individual to which it is issued and allow identification to be verified by both a human and an automated system.

[12] NIST defines multifactor authentication as authentication using two or more factors to achieve authentication. Factors include: (1) something you know (e.g., password or personal identification number); (2) something you have (e.g., cryptographic identification device or token); or (3) something you are (e.g., biometric).

[13] OMB, *Memorandum for the Heads of Executive Departments and Agencies: Continued Implementation of Homeland Security Presidential Directive (HSPD) 12–Policy for a Common Identification Standard for Federal Employees and Contractors*, M-11-11 (Washington, D.C.: Feb. 3, 2011).

However, the Census Bureau did not identify and authenticate all its systems and devices and its implementation of PIV cards was not complete. Specifically,

- Several bureau systems used shared accounts for administrative access, making it more difficult to enforce individual accountability and reconstruct events to support investigations after-the-fact.
- Multiple components of bureau infrastructure and servers did not meet the bureau's minimum password requirements. As a result, there is a heightened risk that unauthorized individuals could exploit these vulnerabilities by guessing a password and using the password to obtain unauthorized access to bureau systems and databases.
- Encryption keys were stored without passwords in certain cases and passwords were not changed as required, increasing the risk that administrator user accounts and passwords could be compromised by attackers.
- Several of the bureau's network devices were configured to use unauthenticated network protocols. Without proper authentication, these protocols can be easily compromised and cause various network disruptions, including network denial of service, unauthorized modification of the network infrastructure, improper routing of network traffic, and issues with logging network data.
- The bureau had not yet completed its implementation of its PIV card system and several cards issued under the bureau's PIV initiative were not PIV-compliant. Bureau project plans indicated that deployment of logical access will not be completed until June 2013. Without a consistent and complete implementation of the PIV standard for both physical and logical access, the bureau increases the risk that its access control systems will not limit access appropriately.

Authorization Controls Were Not Fully Implemented

Authorization is the process of granting or denying access rights and permissions to a protected resource, such as a network, a system, an application, a function, or a file. For example, operating systems have some built-in authorization features such as permissions for files and folders. Network devices, such as routers, have access control lists that can be used to authorize a user who can access and perform certain actions on the device. A key component of granting or denying access rights is the concept of "least privilege." Least privilege is a basic principle for securing computer resources and information. This principle means that a user is granted only those access rights and permissions needed to perform official duties. To restrict legitimate user access to only those programs and files needed to perform work, agencies establish access rights and permissions. “User rights” are allowable actions that can be assigned to a user or to a group of users. File and directory permissions are rules that regulate which users can access a particular file or directory and the extent of that access. To avoid unintentionally authorizing user access to sensitive files and directories, an agency must give careful consideration to its assignment of rights and permissions.

NIST guidance recommends that federal agencies grant a user only the access and rights to information and information systems needed to perform official duties. NSA network security leading practices recommend prohibiting the root account from logging directly into a remote system and creating a set of filtering rules, also known as an access control list, which permits the traffic identified on the list and prohibits other traffic. NSA leading practices also recommend disabling the use of insecure protocols that permit excessive access.

Although the Census Bureau had established an access control requirement based on least privilege and need-to-know principles, the bureau did not always limit user access rights and permissions to only those necessary to perform official duties. For example, unneeded administrative privileges had been granted to certain users on a key bureau infrastructure system and several of the system’s infrastructure devices were also missing access control lists to protect them from potential exploit. Such lists can be used to establish access rules that limit access to resources such as ports used to connect to the network or to a sensitive network used for system administration. However, these lists were not being used on several of the infrastructure devices we reviewed. In addition, the bureau had allowed excessive privileges to default accounts on several databases and used an insecure protocol that permitted excessive access to sensitive system files. The result of these weaknesses is an increased risk of unauthorized access to Census Bureau systems and information.

Strong Encryption Was Not Employed for Several Devices, Databases, and System Components

Cryptography underlies many of the mechanisms used to enforce the confidentiality and integrity of critical and sensitive information. Cryptographic tools help control access to information by making it unintelligible to unauthorized users and by protecting the integrity of transmitted or stored information. A basic element of cryptography is encryption. Encryption is the conversion of data into a form, called a cipher text, which cannot be easily understood. Encryption can be used to provide basic data confidentiality and integrity by transforming plain text into cipher text using a special value known as a key and a mathematical process known as an algorithm. NIST SP 800-53 states that agencies should use encryption to protect the confidentiality of remote access sessions and they should encrypt sessions between host systems. The NIST standard for an encryption algorithm is Federal Information Processing Standards (FIPS) 140-2.[14] NIST SP 800-52[15] also recommends the use of secure socket layer certificates that are signed by a trusted certificate authority, as a means of ensuring authenticity of servers within a network.

However, Census Bureau encryption controls were not consistently implemented in accordance with these guidelines. Specifically,

- Weak password encryption algorithms were used on several devices and for protocols used for the bureau's network. The use of these weak algorithms increases the risk of passwords being compromised by brute force attacks.

- Several databases did not use encryption to appropriately protect data, either while being stored or in transmission. For example, a database containing data collected and protected under Title 13 was not using advanced security features, including encryption, offered by the vendor. Several other databases also were not using encrypted communications. Without encryption, Title 13 data are more susceptible to potential disclosure.

- Components of a bureau system were configured to transmit data without encryption. This creates the possibility of sensitive information being transmitted in clear text across the network, making it susceptible to interception and reuse.

- The bureau made extensive use of secure socket layer certificates as a means of ensuring the authenticity of a server and establishing secure communications with the server. However, the certificates were often invalid or not signed by a trusted certificate authority. As a

[14] NIST, *Security Requirements for Cryptographic Modules*, FIPS 140-2 (Gaithersburg, Md: May, 2001).

[15] NIST, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations, Special Publication 800-52 (Gaithersburg, Md: June, 2005).

result, they cannot be relied on to establish a secure means of communication and the risk is increased that Title 13 data contained in the database could be compromised in transit.

Audit and Monitoring Controls Were Not Fully Implemented

To establish individual accountability, monitor compliance with security policies, and investigate security violations, it is crucial to determine what, when, and by whom specific actions have been taken on a system. Agencies can accomplish this by implementing system or security software that provides an audit trail (a log of system activity) that is used to determine the source of a transaction or attempted transaction and to monitor a user's activities. Audit and monitoring, key components of risk management, involve the regular collection, review, and analysis of auditable events for indications of inappropriate or unusual activity, and the appropriate investigation and reporting of such activity. Automated mechanisms may be used to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities. Use of such mechanisms may enable near real-time continuous monitoring of critical or volatile security controls. Audit and monitoring controls can help security professionals routinely assess computer security, perform investigations during and after an attack, and even recognize an ongoing attack. Audit and monitoring technologies include network and host-based intrusion detection systems, audit logging, security event correlation tools, and computer forensics. NIST guidelines state that agencies should retain sufficient audit logs to allow monitoring of key activities, provide support for after-the-fact investigation of security incidents, and meet agency information retention requirements.

NIST and OMB guidelines emphasize the use of continuous monitoring to improve information security. Continuous monitoring of security controls employed within or inherited by the system is an important aspect of managing risk to information from the operation and use of information systems.[16] The objective of continuous monitoring is to determine if the set of deployed security controls continues to be effective over time in light of the inevitable changes that occur to a system and within an agency. Such monitoring is intended to assist in maintaining an ongoing

[16] According to NIST, the term "continuous" in this context means that security controls and agency risks are assessed, analyzed, and reported at a frequency sufficient to support risk-based security decisions as needed to adequately protect agency information.

awareness of information security, vulnerabilities,[17] and threats[18] to support agency risk management decisions. The monitoring of security controls using automated support tools can help facilitate continuous monitoring.

Although the Census Bureau used various tools to help detect security breaches, such as intrusion detection systems, it did not consistently implement integrated and effective audit and monitoring controls. For example, vulnerability scans of its systems and network devices were performed in an unauthenticated[19] manner, thus limiting the bureau's visibility of system configurations and the usefulness of the scans. The network intrusion detection system also did not cover several key segments of the network and was running at or beyond its design capacity, which causes loss of key forensic data and an inability to detect potential events. Centralized logging of critical network services was not being performed, thus limiting the effectiveness of audit and monitoring activities. In addition, the bureau did not use real-time automated mechanisms to monitor its security posture and check for unauthorized connections of rogue devices to its network. Modern malware can spread in a matter of minutes instead of weeks or months. By not implementing a complete audit and monitoring program, the bureau faces an increased risk that it will not be able to identify weaknesses and remediate them in a timely manner, thus compromising the confidentiality, integrity, and availability of sensitive data. Table 2 describes the status of the bureau's implementation of auditing and monitoring practices.

[17] A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

[18] A threat is any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), assets, individuals, other agencies, or the nation through an information system via unauthorized access, destruction, modification of information, and/or denial of service. Threats to information and information systems include environmental disruptions, human or machine errors, and purposeful attacks.

[19] An authenticated scan uses administrative rights that allow inspection of all security-related elements of network devices, whereas an unauthenticated scan has fewer rights and less visibility.

Table 2: Implementation of Audit and Monitoring Program

Leading practices	Status of implementation	Assessment of Census Bureau efforts
Commerce Department vulnerability scanning and patch management policy requires operating units to perform authenticated vulnerability scanning of network IT assets to allow the scanning device to inspect all security-related elements of each network device.	Partially implemented	Although Census Bureau officials said that they perform compliance scans to monitor network and operating system security, the bureau did not perform authenticated scans of certain network devices, all databases, and systems in certain network segments. Initially, officials said that, due to technical difficulties, they were performing only unauthenticated scans of network devices and did not have the appropriate tools to scan applications and databases. Later, in response to a summary of findings in this report, officials said that they are beginning to deploy additional scans that run in an authenticated mode in several technical environments. In addition, officials said that they are beginning to deploy database and application scans as part of their risk management program; however, they did not provide a deadline for when they will fully implement these scans. As a result, the bureau may not be aware of all vulnerabilities affecting its systems.
NIST guidelines state that intrusion detection systems provide an automated means to monitor events in computer systems and networks to detect, record, and analyze possible computer security incidents.[a] Further, these systems should have the capacity to store key forensic data related to the events to enable investigation, analysis, review, and reporting.	Partially implemented	Although the Census Bureau has partially implemented a network intrusion detection capability, this capability does not cover several key segments of the network. For example, there were insufficient network-based intrusion detection systems to cover the entire agency and no coverage for portions of at least two core networks. Furthermore, the current intrusion detection system infrastructure was running at or beyond its design capacity, which causes loss of key forensic data and an inability to detect potential events.
NIST guidelines state that centralized logging can be of great value in automating the analysis of data and selecting events of interest for human review and recommends maintaining situational awareness of all systems across the agency.	Partially implemented	Although the Census Bureau had a centralized logging system, it did not perform centralized logging of certain critical network services, logins, and network connection activity. As a result, the effectiveness of monitoring, intrusion detection, event correlation, and incident response effectiveness is reduced.

Leading practices	Status of implementation	Assessment of Census Bureau efforts
NIST guidelines state that real-time monitoring of implemented technical controls using automated tools can provide an agency with a much more dynamic view of the effectiveness of those controls and the security posture of the agency.	Partially implemented	Although the Census Bureau's risk-based continuous monitoring plans specified that several scans should be performed weekly, the bureau's monitoring program had only performed monthly scans of systems on its network, and did not perform near real-time continuous monitoring. For example, the bureau had not installed monitoring software (called an agent[b]) on individual computers to enable near real-time monitoring. As an alternative to an agent-based system, officials stated that they plan to deploy network-based compliance scanning; however, the bureau had not yet implemented this scanning process across its IT infrastructure. Additionally, although risk-based continuous monitoring plans called for some scans to be performed weekly, bureau officials stated that scans were being performed monthly, which may not be frequent enough to quickly identify potential threats to the bureau's systems, including systems processing Title 13 data that may contain sensitive personally identifiable information. Officials cited the lack of resources and expertise to implement a robust monitoring program as a significant challenge. However, until the bureau implements a more robust and closer to near real-time monitoring system, either through the use of agents that monitor and report real-time changes or frequent scans of IT assets, it will not have an up-to-date view of security events affecting its systems and thus may have less effective security controls protecting critical computer assets and sensitive information.
Census Bureau IT Security Program Policies[c] require monitoring for unauthorized connections of mobile devices to its information systems.	Not implemented	Although the Census Bureau had a manual process in place for identifying authorized network connections, it did not use mechanisms to monitor for unauthorized connections of mobile devices to its network. For example, officials stated that the Computer Services Division provides information on its own assets to the Office of Information Security using manual updates of an asset list to monitor the status of these assets; however, it was not used to look for unknown assets that might be connected to the network. Officials stated that they were concerned about the impact of such scans on system performance but are considering implementing an automated process. However, they did not provide time frames for doing so. The lack of an effective mechanism to detect and prevent unauthorized devices on bureau networks increases the risk that unauthorized mobile devices could be inadvertently or maliciously connected to the Census Bureau's network, potentially compromising sensitive information.

Source: NIST guidelines and GAO analysis of Census Bureau data.

[a] An incident may have many causes, such as malware (e.g., worms, viruses), attackers gaining unauthorized access to systems from the Internet, and authorized users of systems who misuse their privileges or attempt to gain additional privileges for which they are not authorized.

[b] Agents are programs that run on computers that can monitor and report continuously or periodically on system parameters such as security configurations. Department of Homeland Security guidance recognizes agents as a way of achieving near real-time monitoring capabilities for network resources.

[c] U.S. Census Bureau, *IT Security Program Policies*, version 2.2 (Suitland, Md.: April 2010).

Physical Security Controls Weaknesses Expose Bureau Resources to Potential Accidental or Malicious Damage

Physical security controls are a key component of limiting unauthorized access to sensitive information and information systems. These controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. They include restricting physical access to computer resources and sensitive information, usually by limiting access to the buildings and rooms in which the resources are housed and periodically reviewing access rights to ensure that access continues to be appropriate based on established criteria. Such controls include perimeter fencing, surveillance cameras, security guards, gates, locks, and environmental controls such as smoke detectors, fire alarms and extinguishers, and uninterruptible power supplies. NIST guidelines state that federal agencies should implement physical security and environmental safety controls to protect employees and contractors, information systems, and the facilities in which they are located. Furthermore, the Interagency Security Committee[20] issues baseline sets of security measures to be implemented at all federal facilities. These baselines provide guidance to agencies on how to protect parking areas, monitor agency facilities, and identify authorized personnel.

The Census Bureau did not fully implement all applicable guidance for physical security of its information resources. The bureau did demonstrate effective physical security in several cases, including screening of visitor vehicles, intrusion detection, closed circuit television coverage, and a policy requiring the use of badges. However, implementation of these measures was not consistent across all of the facilities that we reviewed. For example, one facility routinely disabled the use of access readers, potentially allowing unauthorized access to the Census Bureau's network and phone systems. This and other weaknesses could expose Census Bureau information resources to accidental or malicious damage, and result in the loss of protected data.

[20] The ISC was established pursuant to Executive Order 12977, October 19, 1995, "Interagency Security Committee," as amended by Executive order 13286, March 5, 2003. According to the ISC, the first set of governmentwide physical security standards for federal facilities was established pursuant to the Vulnerability Assessment of Federal Facilities issued by the U.S. Department of Justice in 1995. The ISC, established after the issuance of the assessment, addressed these standards and has issued additional security standards for buildings that are under construction or major modification, as well as for lease acquisitions.

Weaknesses in Other Important Controls Increase Risk

In addition to access controls, other important controls should be in place to ensure the confidentiality, integrity, and availability of an agency's information. These controls include policies, procedures, and techniques to (1) manage and implement system configurations, and (2) establish plans for contingencies if normal operations are disrupted. Weaknesses in these areas could increase the risk of unauthorized use, disclosure, modification, or loss of the Census Bureau's mission-sensitive information.

Configuration Management Weaknesses Found in Patch Management and Device Configuration

Configuration management controls ensure that only authorized and fully tested software is placed in operation, software and hardware are updated, patches are applied to these systems to protect against known vulnerabilities, and changes are documented and approved. To protect against known vulnerabilities, effective procedures must be in place, appropriate software installed, and patches updated promptly. Up-to-date patch installation helps mitigate flaws in software code. An information system with inadequate configuration management controls is at an increased risk of facing significant damage and may enable malicious individuals to exploit system vulnerabilities.

The Census Bureau has documented policies and procedures for managing and implementing configuration management settings for its systems, including a policy for establishing secure configuration standards for bureau systems. However, the bureau did not always implement configuration management controls. For example, patch management practices lacked centralized oversight and control to effectively administer patches and several database servers had not been patched or were running outdated software. In addition, key communication systems were not securely configured and did not have FIPS 140-2-validated encryption and network devices were configured in a way that allowed unencrypted logins, which could allow user IDs and passwords to be compromised. Further, the bureau had not implemented the routine monitoring of its configurations for its infrastructure applications and did not document emergency changes before making them. According to the bureau, changes are verbally approved and then documented after implementation. Without proper implementation of configuration management policies and procedures and adequate security controls, the bureau's systems are susceptible to many known vulnerabilities.

Contingency Planning Did Not Incorporate All Guidelines

Contingency planning helps ensure that if normal operations are interrupted, network managers are able to detect, mitigate, and recover from a service disruption while preserving access to vital information.

Contingency plans detail emergency response, backup operations, and disaster recovery for information systems. These plans should be clearly documented, communicated to potentially affected staff, updated to reflect current operations, and regularly tested. NIST guidelines state that the criticality and sensitivity of computerized operations and IT resources must be predetermined. NIST guidelines also recommend that agencies develop, document, and implement plans and procedures to support contingency planning, such as a continuity of operations plan, for information systems that support the agency's operations and assets.

The Census Bureau has satisfied several, but not all NIST contingency planning practices. For example, the bureau provided evidence that it had taken steps to actively mitigate disruptions to its primary data center through the implementation of emergency power, fire suppression, and flood mitigation measures. Additionally, the bureau stored backup copies of data for its critical systems off site at a secured location. However, the Census Bureau did not satisfy many of the other practices for contingency planning. Without an effective and complete contingency plan, an agency's likelihood of recovering important systems in a timely manner is diminished. Table 3 describes the status of the bureau's implementation of several of the bureau's contingency planning practices.

Table 3: Census Contingency Planning Practices

Leading practices (based on NIST guidelines)	Status of implementation	Assessment of Census Bureau efforts
Contingency plans for information systems should include priorities for restoring systems.	Not implemented	The Census Bureau had not established restoration priorities for bureau information systems or processing functions in its contingency plans. For example, the contingency plan stated that staff will meet following a disaster and will prioritize functions at that time. According to the Chief Information Security Officer, this occurs because employees for each system are responsible for developing contingency plans for that system. Assessment and prioritization of recovery activities provide the foundation of an agency's security plan. By not prioritizing activities before an incident, the bureau is increasing the risk that the bureau may not be able to sustain business functions if an incident occurs.

Leading practices (based on NIST guidelines)	Status of implementation	Assessment of Census Bureau efforts
Contingency plans should be distributed to key personnel, account for primary and alternate contact methods, and discuss procedures to be followed if an individual cannot be contacted.	Partially implemented	The contingency plan for the Bowie Computing Center was missing critical information that would be necessary during a disaster. The plan addressed roles and responsibilities for key personnel and included provisions for the plan to be distributed to key personnel; however, the plan did not contain contact information and information on backup personnel. Furthermore, the Alternate Disaster Recovery Coordinator stated that she did not have a copy of the plan and was unaware of anyone who did. According to the Chief Information Security Officer, there is no process for ensuring and verifying that identified staff members have copies of documentation stored off site. The lack of key information and off-site copies of the plan increases the risk that the plans will not be available in the event of a disaster.
Disaster testing should include identifying potential weaknesses to determine the plan's effectiveness and the organizations readiness to execute the plan.	Partially implemented	Although the Census Bureau conducted annual disaster testing to determine its disaster recovery plan's effectiveness and organizational readiness, the testing did not comprehensively test for potential weaknesses. The bureau uses the same employees each year to perform the testing and tests the restoration of the same system, and only that system, each year. According to officials, the bureau uses the same system every year because it has a wide range of infrastructure supporting it, which makes the system ideal for testing. Unless the bureau uses a broader pool of employees and systems, it will not be able to assess weaknesses in how well employees have been trained to carry out their roles and responsibilities in a disaster situation. Furthermore, without alternating the systems that are being restored, the bureau will not know if there are weaknesses in their other system recovery plans.

Source: NIST guidelines and GAO analysis of Census Bureau data.

Census Bureau Has Not Implemented All Elements of Its Information Security Program

A key reason for the weaknesses in controls over the Census Bureau's information and information systems is that it has not yet implemented all elements of its agencywide information security program to ensure that controls are effectively established and maintained. FISMA requires each agency to develop, document, and implement an information security program that, among other things, includes:

- periodic assessments of the risk and the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems;

- policies and procedures that (1) are based on risk assessments, (2) cost-effectively reduce risks, (3) ensure that information security is addressed throughout the life cycle of each system, and (4) ensure compliance with applicable requirements;

- security awareness training to inform personnel of information security risks and their responsibilities in complying with agency policies and procedures and information security training for personnel who have significant security responsibilities for information security; and

- procedures for detecting, reporting, and responding to security incidents.

Weaknesses in an information security program could increase the risk that emerging security weaknesses will not be identified and that sensitive information and assets will not be adequately safeguarded from inadvertent or deliberate misuse, improper disclosure, or destruction.

Census Bureau Is Implementing New Risk Management Program, but Several Risk-Based Decisions Were Not Fully Documented

NIST guidelines[21] call for agencies to develop a risk management framework with the goal of embedding security in the culture and systems of that agency instead of using a point-in-time tool for compliance. That framework should include an assessment of the impact those risks could have on organizational operations and an analysis of the acceptable level of risk under which the agency could absorb the resulting loss while still maintaining operation of its systems (a risk impact analysis). In addition, to monitor the effectiveness of its security controls, the agency should conduct a vulnerability assessment of its systems to ensure that security requirements for the system are being met. The results of the risk impact analysis and the effectiveness of security controls should be documented. Finally, NIST and OMB specify that federal agencies should develop remedial action plans, also known as plans of action and milestones (POA&M) that describe specific tasks and milestones for correcting security weaknesses in information systems and are used to set priorities and monitor progress in correcting the weaknesses.

The bureau's risk management program emphasizes the following capabilities:

- Risk profiles/scoring— Risk profiles are developed based on standardized questionnaires containing business and technological factors, and a risk scoring methodology to identify appropriate security controls and determine the level of risk for each control. Profiles are to incorporate the content of the system security plan and risk assessment into a single, quantitative measure of risk to facilitate risk-based decisions.

[21] NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems*, Special Publication 800-37, Revision 1 (Gaithersburg, Md.: February 2010).

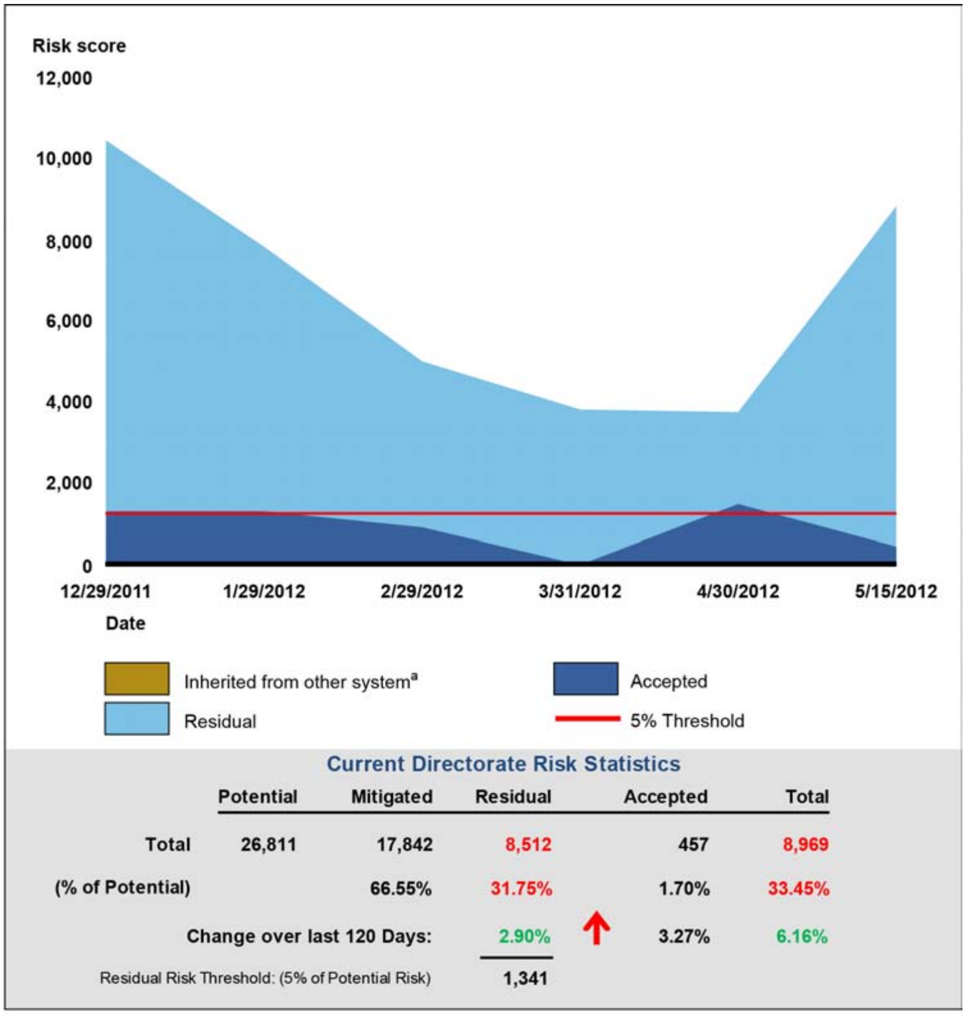
- Automation—The use of automated assessments to consistently and repeatedly assess Census Bureau information systems against organizational benchmarks.

- Integration with the software development life cycle—Consideration of security during system design and development to reduce postdeployment security-related changes.

- Reporting—Providing routine reports to management, system owners, and authorizing officials quantifying the risk for a given information system, including potential risk, mitigated risk, risk accepted by the authorizing official, and the residual risk for the system.

Figure 3 is an example of a report generated under the new program. It shows the status of various elements in the bureau's risk management program.

Figure 3: Example of a Report Generated from the Census Bureau's Risk Management Program



Current Directorate Risk Statistics

	Potential	Mitigated	Residual		Accepted	Total
Total	26,811	17,842	8,512		457	8,969
(% of Potential)		66.55%	31.75%		1.70%	33.45%
Change over last 120 Days:			2.90%	↑	3.27%	6.16%
Residual Risk Threshold: (5% of Potential Risk)			1,341			

Source: Census Bureau documentation.

[a] Inherited from other system data was not available at this time.

According to bureau officials, implementation of the new program will increase the emphasis on real-time monitoring of information systems, allow the bureau to prioritize limited resources to address security vulnerabilities, and provide improved awareness by bureau management of information security risks through routine and more easily understandable reporting.

While the bureau’s new program may produce these benefits, it does not yet present a complete picture of the risks to Census Bureau systems. Specifically, the bureau’s policies and NIST guidelines direct the bureau to consider both individual system controls and common controls (controls shared by multiple systems) in assessing system risk. However, the bureau’s security assessment report for its pilot system did not include an assessment of the risks associated with the specified common controls; instead, it stated that the data were not finalized and not available. Census Bureau officials said that the assessment of the common controls had not been completed under the new strategy, and thus was not reflected in the security assessment report for the system. Until the bureau clearly documents its assessment of common controls for its information systems, it may not have an accurate understanding of the risks these systems are subject to.

In addition, although the Census Bureau’s system security plans listed more than 1,200 security controls for each of the seven components of the pilot system, the assessments of those controls and the related security assessment report did not fully identify and document several vulnerabilities identified during our review. For example, the bureau was not fully enforcing session inactivity time outs for remote users and was allowing remote users to simultaneously access internal bureau networks and the Internet. Risks for these vulnerabilities were not accepted in the security assessment report used to authorize operation of the system, although the time out vulnerability was identified and accepted in a later document.

Furthermore, documentation supporting both risk-based decisions and closure of remediation plans was missing or unclear. Both NIST and Census Bureau guidance state the importance of documenting in sufficient detail whether implementation of a control effectively addresses the control requirement and the rationale for any accepted risks. However, the bureau’s documentation of key decisions was not always available, clear and complete. For example, we reviewed seven system security plans for seven pilot system components and identified 48 cases where security controls did not pass their respective control assessments, known as exceptions. Of these exceptions, the bureau chose to accept 23 exceptions and attempted to remediate 25. Of the 23 exceptions the bureau chose to accept, documentation was not provided for 7.

For the 25 exceptions the bureau attempted to remediate, the bureau initially created a POA&M for each exception to monitor the progress in correcting the weaknesses. Five of these POA&Ms remained open as of

May 2012 and 20 had been closed. However, 17 of the 20 closed POA&Ms did not have documentation that demonstrated that the weaknesses had been addressed. For example, the documentation for 6 of the closed POA&Ms stated that integrity scans had been performed to address the weaknesses but the supporting evidence did not indicate that the scans had been completed. Census Bureau officials stated that the authorizing official for the pilot system chose to accept the risk from these weaknesses, but this had not been documented as part of the POA&M closure. In addition, 11 of the 20 closed POA&Ms were closed because the risk was accepted and approved by the system owner, information security representative, and authorizing official on a risk acceptance form but there was no evidence documented that mitigating controls were in place. In many cases, the bureau listed compensating controls in the risk acceptance form that mitigated the risk, but did not provide evidence that it had tested these compensating controls to assess their effectiveness. For example, an exception related to encryption stated that the system relied on the underlying operating system and network infrastructure to mitigate the issue but did not clearly explain how this was to occur.

While the bureau's new program for risk management may produce potential benefits to the bureau, the effectiveness of its remediation efforts cannot be known unless the bureau ensures that its actions have been documented.

Security Management Program Policies Were Documented, but Were Out of Date

An entitywide information security management program is the foundation of a security control structure and a reflection of senior management's commitment to addressing security risks. Per FISMA, the security management program should establish a framework and a continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, or improperly implemented; and controls may be inconsistently applied.

The Census Bureau's 2010 IT Security Program Policies referenced the 18 control areas that address FISMA requirements for a security management program at a high level, with the intent that detailed guidance and requirements are included in the underlying system-level documentation, according to bureau officials. However, although the bureau requires that its IT security program and policies be revised at least annually, it has not been updated since April 2010. According to bureau officials, a revision had been drafted, but its approval had been delayed, in part due to the bureau's efforts to implement its new risk management framework. Until the Census Bureau's IT Security Program Policies are updated and finalized, the bureau may not have assurance that controls over its information are appropriately applied to its systems and operating effectively.

Security Awareness and Training Procedures Were Documented, but Training Was Not Tracked or Delivered for Many Users

FISMA mandates that federal employees and contractors who use agency information systems that support agency operations and assets be provided with training in information security awareness. Furthermore, OMB guidance states that personnel should have this training before they are granted access to systems or applications. According to FISMA and OMB, the information security awareness training should inform personnel, including contractors and other users of information systems supporting the operations and assets of an agency, of information security risks associated with their activities and their roles and responsibilities to properly and effectively implement the practices that are designed to reduce these risks. FISMA also includes requirements for training personnel who have significant responsibilities for information security. Depending on an employee's specific security role, training could include specialized topics such as incident detection and response, physical security, or firewall configuration. NIST SP 800-53 Rev. 3 further recommends that agencies require refresher training for security awareness and role-based on an agency-defined basis, and document users' completion of required training. In addition, Census Bureau policy requires all personnel to complete annual security awareness training and those personnel with significant network security roles and responsibilities to complete sufficient information system security training and continuing education to ensure compliance with agency policy.

Table 4 describes the implementation status of the bureau's information security awareness and training practices. While the Census Bureau has developed and documented awareness and training policies and procedures, not all users who should have completed security awareness or role-based training did so, and the bureau's training database did not track security awareness activities for all users. Until the Census Bureau tracks security awareness activities and enforces the completion of security awareness and role-based training for all users, the bureau does not have reasonable assurance that its employees have the adequate knowledge, skills, and abilities consistent with their roles to protect the information housed within bureau systems to which they are assigned.

Table 4: Census Information Security Awareness and Training Practices

Leading practices (from NIST SP 800-53 Rev. 3)	Status of implementation	Assessment of Census Bureau efforts
The agency has current, formal, documented awareness and training policies and procedures.	Implemented	The Census Bureau had current, formal, documented security awareness and training policies and procedures.
The agency must document and retain training records in accordance with an organizationally-defined time period.	Partially implemented	The Census Bureau does not track training for all bureau employees. Its database of record did not track whether its estimated 5,500-6,000 field representatives had completed the required annual security training. The bureau reported that in fiscal year 2011, training for field representatives was tracked by individual regional offices, rather than in the centralized training database. However, the bureau did not provide evidence of this tracking for review. In addition, the bureau does not track whether Office of Information Security employees have completed their initial role-based training. As a result, the bureau's ability to determine the extent to which its employees have completed the required security awareness training was limited. The bureau stated that as of fiscal year 2012, training for all employees was being tracked in the database of record, although the agency had not provided evidence that this process had been fully implemented.
The agency provides basic security awareness training to all users as part of initial training, and refresher training to all users on an agency-defined basis thereafter.	Partially implemented	Census Bureau records show that not all of its employees have successfully completed the required awareness training during fiscal year 2011. Of the personnel tracked in the database of record, the bureau estimated 88 percent had completed the required awareness training in fiscal year 2011. However, as noted, bureau officials estimated that between 5,500 and 6,000 employees were not tracked in the database, and were unable to provide information on how many of those personnel had completed the required awareness training. As a result, the bureau has less assurance that its personnel have a basic awareness of information security issues and agency security policies and procedures. Bureau officials stated they were unable to enforce the annual security awareness training requirement due to a dispute with the agency's employee union.
The agency provides role-based training to designated users as part of initial training, and refresher training on an agency-defined basis thereafter.	Partially implemented	Two of five Census Bureau system owners and authorizing officials who should have received initial training in fiscal year 2011 did not. Additionally, 6 of 17 authorizing officials and system owners did not complete the required annual training in fiscal year 2011, and 6 of 33 individuals who were required to hold professional certifications had not been certified. Office of Information Security officials said that their ability to enforce training requirements on personnel in divisions other than the Office of Information Security was limited, due to the training's cost, which must be paid by the other divisions. As a result, the bureau has less assurance that some system owners and authorizing officials have the necessary skills and knowledge to effectively perform their functions.

Source: NIST guidelines and GAO analysis of Census Bureau data.

Incident Response Policies and Procedures Were Generally Developed and Documented, but Were Not Fully Implemented

Incident response controls are necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.[22] While strong controls may not prevent all incidents, agencies can reduce the risks associated with these events by detecting and promptly responding before significant damage is done. Agencies should create an incident response policy and use it as the basis for incident response procedures. The ability to identify incidents using appropriate audit and monitoring techniques enable an agency to initiate its incident response plan in a timely manner. Once an incident has been identified, an agency's incident response processes and procedures should provide the capability to correctly log the incident, properly analyze it, and take appropriate action.

Table 5 shows the status of the bureau's implementation of incident response practices. While the Census Bureau had policies and procedures for handling information security incidents in place, including developing a process of preparation, detection, analysis, containment, eradication, and recovery, it had only partially implemented them. Without effective processes and procedures, the bureau will have greater difficulty in detecting incidents, minimizing the resultant loss and destruction, mitigating the exploited weaknesses and restoring services.

Table 5: Census Incident Response Practices

Leading practices (from NIST SP 800-53 Rev. 3 unless otherwise noted)	Status of implementation	Assessment of Census Bureau efforts
The agency has current, documented incident response policies and procedures.	Implemented	The bureau had current, documented incident response policies and procedures.
The agency provides initial and refresher incident response training to personnel who have incident response roles and responsibilities. Department of Commerce policy requires personnel in specialized security positions such as incident response to hold related professional certifications to meet this requirement.	Partially implemented	Four of six incident response personnel did not hold the required professional certifications. The bureau stated that a number of training classes had been cancelled, interrupting its employees' training plans. As a result, the bureau has reduced assurance that its incident response personnel have the necessary skills to carry out their responsibilities.

[22] See, for example, NIST, *Computer Security Incident Handling Guide,* Special Publication 800-61, Revision 1 (Gaithersburg, Md., March 2008).

Leading practices (from NIST SP 800-53 Rev. 3 unless otherwise noted)	Status of implementation	Assessment of Census Bureau efforts
The agency evaluates the effectiveness of the incident response capability, using organizationally-defined tests or exercises, at a specified frequency.	Partially implemented	The bureau held annual incident response plan testing, but the tests lacked plans and criteria, and the bureau did not evaluate the effectiveness of the incident response capability. Census Bureau officials stated that they lack formal processes for evaluating the effectiveness of the Census Bureau's Computer Incident Response Team in tests and exercises. As a result, the bureau has reduced assurance that its incident response plan will be operable in the case of a major incident.
The agency implements an incident handling capability that includes preparation, detection and analysis containment, eradication and recovery, and tracks and documents information security incidents.	Partially implemented	The bureau took steps to prepare for and detect information security incidents. For the 24 incidents we reviewed in depth, incident handlers analyzed possible incidents, but did not prioritize them based on current or potential effects and the criticality of the affected resources. Additionally, for 8 of the 24 incidents we reviewed, the bureau did not document in the incident log whether it had conducted containment and/or eradication and recovery actions. Officials stated that Computer Incident Response Team had addressed the incidents, but some relevant information included in e-mail conversations and tickets in the system used to track workstation repair and maintenance requests had not been documented in the incident tracking database. As a result, the bureau has less assurance that its incident handlers will be able to use the incident log as a coordination tool and source of situational awareness information.
The agency develops an incident response plan that details how to implement the incident response capability, shows how incident response fits into the overall organization, meets the agency's unique requirements, defines reportable incidents, provides metrics for evaluating the incident response capability, defines the resources and management support necessary to develop and maintain the incident response capability, and is reviewed and approved by designated officials within the organization.	Partially implemented	The bureau's incident response plan showed how the incident response capability fits into the agency's organization, how to implement incident response, defines reportable incidents, and is reviewed and approved by designated officials. However, it did not define the necessary resources and management support to maintain the incident response capability or identify unique requirements that the incident response capability needs to meet. Although it was not detailed in the plan, officials from the Office of Information Security said that the office measured its effectiveness by metrics such as the timeliness of reporting incidents involving personally identifiable information or laptop loss to the Department of Commerce and the US-Computer Emergency Readiness Team (US-CERT) and the number of incidents by category opened each month as metrics to measure the Computer Incident Response Team's effectiveness. However, they did not provide examples of such reporting for review. As a result, the bureau cannot be sure that its incident response is effectively meeting its unique needs.

Leading practices (from NIST SP 800-53 Rev. 3 unless otherwise noted)	Status of implementation	Assessment of Census Bureau efforts
The agency requires personnel to report suspected security incidents to the incident response capability within a defined time period, and reports security incident information to designated authorities. OMB policy requires all federal agencies to report incidents to US-CERT within specified time frames.	Partially implemented	The bureau's policy required personnel to report incidents involving personally identifiable information incidents to the Computer Incident Response Team within 1 hour, and all other incidents with 24 hours. For the 24 incidents we reviewed in depth, the bureau did not report 9 of 16 reportable incidents to US-CERT; officials said they only occasionally report incidents not involving personally identifiable information to US-CERT. Additionally, bureau officials stated that not all incidents were properly classified according to US-CERT guidelines. Bureau officials stated the Computer Incident Response Team has focused on reporting high-impact events involving personally identifiable information and lost laptops to US-CERT, with less emphasis on other categories of incidents. Additionally, officials stated that the bureau relies on automatic classification of events based on individual responses on the incident submission form, rather than incident handler analysis, to classify incidents. As a result of not reporting all incidents to US-CERT, the organization does not have a complete picture of the number and type of information security incidents that Census Bureau is encountering.
NIST SP 800-61 guidelines state that agencies should strive to detect and validate malware incidents rapidly.	Partially implemented	Of the 4 malware incidents among the 24 selected for in-depth review, 2 were identified as a false positive, and a detection before infection, respectively, while a third was unresolved, with a forensic analysis of the suspect machine still pending more than 8 months after the initial incident report, and the fourth was closed with no information indicating whether a planned forensic examination had been performed. Census Bureau officials stated that the bureau is still building its digital forensics capability and the availability of staff with the necessary skills is limited. As a result, the bureau has a reduced ability to minimize the impact of malware incidents through rapid response.
The agency implements an incident handling capability for security incidents that incorporates lessons learned from ongoing incident handling activities into training, testing, and procedures. In addition, Census Bureau policies require its Computer Incident Response Team to take advantage of lessons learned from incident handling.	Not implemented	Census Bureau officials stated that, while they attempt to identify patterns in incidents as they occur, they do not have a process to formally review incidents to identify opportunities for improvement. As a result, the bureau's ability to learn from ongoing activities and improve its incident handing capability is reduced.

Source: NIST guidelines, Department of Commerce policy, and GAO analysis of Census Bureau data.

Conclusions

The Census Bureau has taken important steps in implementing controls to protect the information and systems that support its mission. However, significant weaknesses in access controls and other information security controls exist that impair its ability to ensure the confidentiality, integrity, and availability of the information and systems supporting its mission. A key reason for many of the weaknesses is that the bureau has not yet fully implemented elements of its information security program to ensure that effective controls are established and maintained. Effective implementation of such a program includes comprehensively assessing risk, establishing appropriate policies and procedures, providing security awareness training, and responding to incidents. Until the bureau addresses identified control weaknesses and fully implements its information security program, it will have limited assurance that its information and information systems are adequately protected against unauthorized access, disclosure, modification, or loss.

Recommendations for Executive Action

To fully implement its agencywide information security program, we recommend that the Acting Secretary of Commerce direct the Under Secretary for Economic Affairs who oversees the Economics and Statistics Administration and the Acting Director of the U.S. Census Bureau to implement the following 13 recommendations.

1. Clearly document the bureau's assessment of common controls for information systems before granting an authorization to operate.
2. Clearly document acceptance of risks and remedial actions for management review and approval before closing them.
3. Establish a deadline for updating and finalizing the bureau's IT Security Program Policies document.
4. Fully implement the bureau's new process for tracking employee completion of security awareness training in the database of record.
5. Enforce the requirement for annual security awareness training for all users and ensure all users complete the training.
6. Enforce the requirement that all individuals with significant security responsibilities complete both initial and refresher role-based training.
7. Provide sufficient opportunities for incident response personnel to complete required training and certifications and verify compliance.
8. Develop plans and criteria or metrics for incident response plan tests and exercises, and evaluate the effectiveness of the incident response capability.
9. Verify that incident response personnel document in the incident log the actions taken to contain, eradicate, and recover from incidents.
10. Fully develop an incident response plan by documenting metrics used for measuring the bureau's incident response effectiveness and defining the resources and management support necessary to

develop an incident response capability that meets the Census Bureau's unique needs.

11. Ensure that all reportable incidents are reported to US-CERT.
12. Complete development of a mature digital forensics capability to better detect and validate malware incidents.
13. Develop a process to formally review incidents, gather lessons learned from ongoing incident handling activities and incorporate identified improvements into training, testing, and procedures.

In a separate report with limited distribution, we are making 102 recommendations to address the technical weaknesses related to access controls, configuration management, and contingency planning that we identified.

Agency Comments and Our Evaluation

The Acting Secretary of Commerce provided written comments from the bureau on a draft of this report on January 2, 2013 (reprinted in app. II). In its comments, the Census Bureau expressed broad agreement with the overall theme of the report but did not directly comment on the recommendations. The bureau stated that it is putting together a team from throughout the organization to carefully review each finding and prepare a specific course of action to address them. However, it raised concerns about four specific aspects of the summary of findings which GAO addressed as appropriate.

Specifically, with respect to our draft finding that the bureau had not updated and finalized its IT security program and policies document since April 2010, the bureau stated that subsequent to our field work ending in September 2012, its updated policy document was published in October 2012. The bureau stated that our finding should state that its policy is to be revised every other year, instead of annually as stated in the draft, but did not provide written documentation to support this statement. The Census Bureau's IT Security Program Policies document, dated April 2010, that we were provided for review stated in the program management control family, which is applicable to the information security requirements for the bureau as a whole, that review and revision of the Census Bureau's information security program plan and certain supporting policies be done annually. Accordingly, we believe our report is accurate. Further, we believe the actions taken by the bureau meet the intent of our recommendation which was to establish a deadline for updating and finalizing the bureau's IT Security Program Policies document.

With respect to our draft finding that the bureau's security assessment report for its pilot system did not include an assessment of the risks associated with the specified common controls, and that the data was not finalized or available, the bureau acknowledged that results of an assessment of the common controls were not presented on the risk assessment report that was provided to the authorizing official in the new risk management framework format. However, the bureau stated that it had assessed the common controls. We did not intend to imply that the bureau had not conducted an assessment of common controls only that it was not included in the security assessment report. Accordingly, we have clarified our language and recommendation in the report to better reflect this scenario.

Regarding our draft finding that the bureau's continuous monitoring program did not include mechanisms for near real-time continuous monitoring, the bureau stated that the frequency at which it performs scans is based on the identified risk of the control or system being assessed, and that monthly scans were consistent with the risk level it had identified for Title 13 data. However, this statement is inconsistent with the risk-based continuous monitoring plans that we were provided by the bureau during our review, which called for weekly scanning in several cases. Furthermore, NIST guidelines note the importance of near real-time data as an input to an agency's security decision-making process, and the bureau's risk management framework documentation noted that near real-time risk monitoring is a long-term goal for the bureau. We have clarified our finding to better reflect the bureau's continuous monitoring plans.

Finally, in responding to our draft finding that the bureau did not provide a deadline for when it would fully implement database and application scans, the bureau stated that it had provided a schedule during our fieldwork and subsequently provided another schedule intended to clarify those deadlines. However, upon review of the new schedule, it did not address deadlines for implementing database and application scans. As a result, we believe the finding is valid.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution of it until 30 days from the date of this letter. At that time, we will send copies to the Acting Secretary of Commerce, the Acting Director of the U.S. Census Bureau, and interested congressional committees. In addition, the report will be available at no charge on GAO's website at http://www.gao.gov.

If you have any questions about this report, please contact Gregory C. Wilshusen at (202) 512-6244 or Dr. Nabajyoti Barkakati at (202) 512-4499. We can also be reached by e-mail at wilshuseng@gao.gov or barkakatin@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix III.

Sincerely yours,

Gregory C. Wilshusen

Gregory C. Wilshusen
Director, Information Security Issues

Nabajyoti Barkakati

Dr. Nabajyoti Barkakati
Chief Technologist

Appendix I: Objective, Scope, and Methodology

The objective of our review was to determine whether the Census Bureau effectively implemented appropriate information security controls to protect the confidentiality, integrity, and availability of the information and systems that support its mission.

To determine the effectiveness of the bureau's security controls, we gained an understanding of the overall network control environment, identified interconnectivity and control points, and examined controls for the agency's networks and facilities. Specifically, we reviewed controls over the bureau's network infrastructure and systems that support its handling of information collected and protected pursuant to Title 13. We performed our work at the bureau headquarters in Suitland, Maryland, at the Bowie Computing Center in Bowie, Maryland, and at the National Processing Center in Jeffersonville, Indiana.

We selected 12 systems for review. We initially focused on systems that contained Title 13 data screened for public release as well as systems that had private or potentially sensitive data. However, during our review, we discovered that some systems included portions of others due to the interconnected nature of the bureau's environment, so we included those systems in our scope as well.

To evaluate the bureau's controls over its information systems, we used our *Federal Information System Controls Audit Manual*,[23] which contains guidance for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized information; National Institute of Standards and Technology (NIST) standards and guidelines; bureau policies, procedures, practices, and standards; and standards and guidelines from relevant security and IT security organizations, such as the National Security Agency, Center for Internet Security, and Interagency Security Committee. Where applicable, we assessed the status according to how completely the bureau's policies and practices aligned with the guidance. In these cases, we assigned ratings of "implemented", "partially implemented", or "not implemented" based on that assessment. A rating of "partially implemented" was given if the bureau's activities satisfied at least one component of the relevant standards and guidelines.

[23] GAO, *Federal Information System Controls Audit Manual (FISCAM)*, GAO-09-232G (Washington, D.C.: February 2009).

Specifically, we

- reviewed network access paths to determine if boundaries had been adequately protected;
- reviewed the complexity and expiration of password settings to determine if password management was being enforced;
- analyzed users' system authorizations to determine whether they had more permissions than necessary to perform their assigned functions;
- observed configurations for providing secure data transmissions across the network to determine whether sensitive data were being encrypted;
- reviewed software security settings to determine if modifications of sensitive or critical system resources had been monitored and logged;
- reviewed the Census Bureau's implementation of continuous monitoring and use of automated tools to determine the extent to which it uses these tools to manage IT assets and monitor the security configurations and vulnerabilities for its IT assets;
- observed physical access controls to determine if computer facilities and resources were being protected from espionage, sabotage, damage, and theft;
- examined configuration settings and access controls for routers, network management servers, switches, and firewalls;
- inspected key servers and workstations to determine if critical patches had been installed and/or were up to date; and
- examined polices, and procedures, and implementation of controls related to segregation of duties.

Using the requirements identified by the Federal Information Security Management Act of 2002, which establishes key elements for an effective agencywide information security program, and associated NIST guidelines and bureau requirements, we evaluated the Census Bureau's information security program by:

- analyzing processes and documentation that were part of the bureau's new risk management framework implementation to determine the extent to which it accurately characterized information security risks;

- analyzing bureau policies, procedures, practices, and standards to determine their effectiveness in providing guidance to personnel responsible for securing information and information systems, including areas such as segregation of duties;

- examining the security awareness training process for employees and contractors to determine whether they had received training according to federal requirements;

- examining training records for personnel who have significant responsibilities to determine whether they had received training commensurate with those responsibilities; and

- reviewing bureau policies and procedures and a selection of information security incidents to determine the extent to which bureau incident handling practices complied with applicable NIST guidelines and federal requirements. We selected 24 incidents for detailed review based on our initial examination of 1,015 incidents that the bureau logged between Jan. 4, 2010 and Feb. 8, 2012. We selected a non-generalizable, judgmental sample of 8 incidents from each of the following 3 categories: incidents still open, incidents closed based on information not in the log, and incidents which, based on the log data, appeared as if they may not have been handled in accordance with bureau policies or procedures or NIST guidelines.

As part of our review of the bureau's agencywide information security program, we reviewed several sources of computer-generated data. These included the bureau's:

- inventory of information systems,

- plans of action and milestones for identified information security weaknesses,

- annual IT security training completion data,

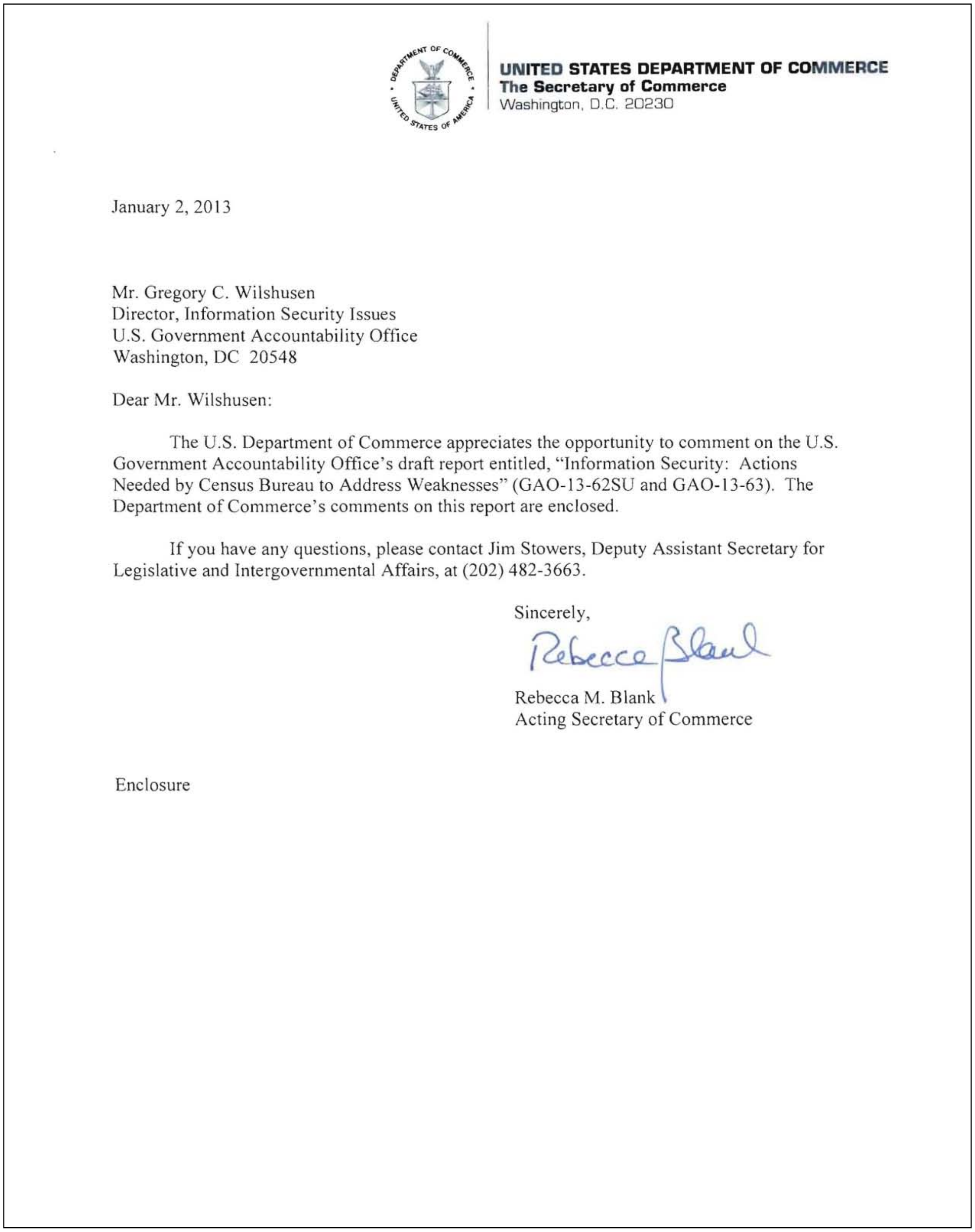
- role-based training for individuals with significant security responsibilities, and

- log of information security incidents.

To verify the reliability of the data in these systems, we examined it for obvious outliers, omissions, and errors. We also verified a selection of individual records for accuracy and completeness, and verified our analysis of the information with agency officials. We determined that these sources of data were sufficiently reliable for our purposes.

We conducted this performance audit from January 2012 through January 2013 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Department of Commerce



UNITED STATES DEPARTMENT OF COMMERCE
The Secretary of Commerce
Washington, D.C. 20230

January 2, 2013

Mr. Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
Washington, DC 20548

Dear Mr. Wilshusen:

The U.S. Department of Commerce appreciates the opportunity to comment on the U.S. Government Accountability Office's draft report entitled, "Information Security: Actions Needed by Census Bureau to Address Weaknesses" (GAO-13-62SU and GAO-13-63). The Department of Commerce's comments on this report are enclosed.

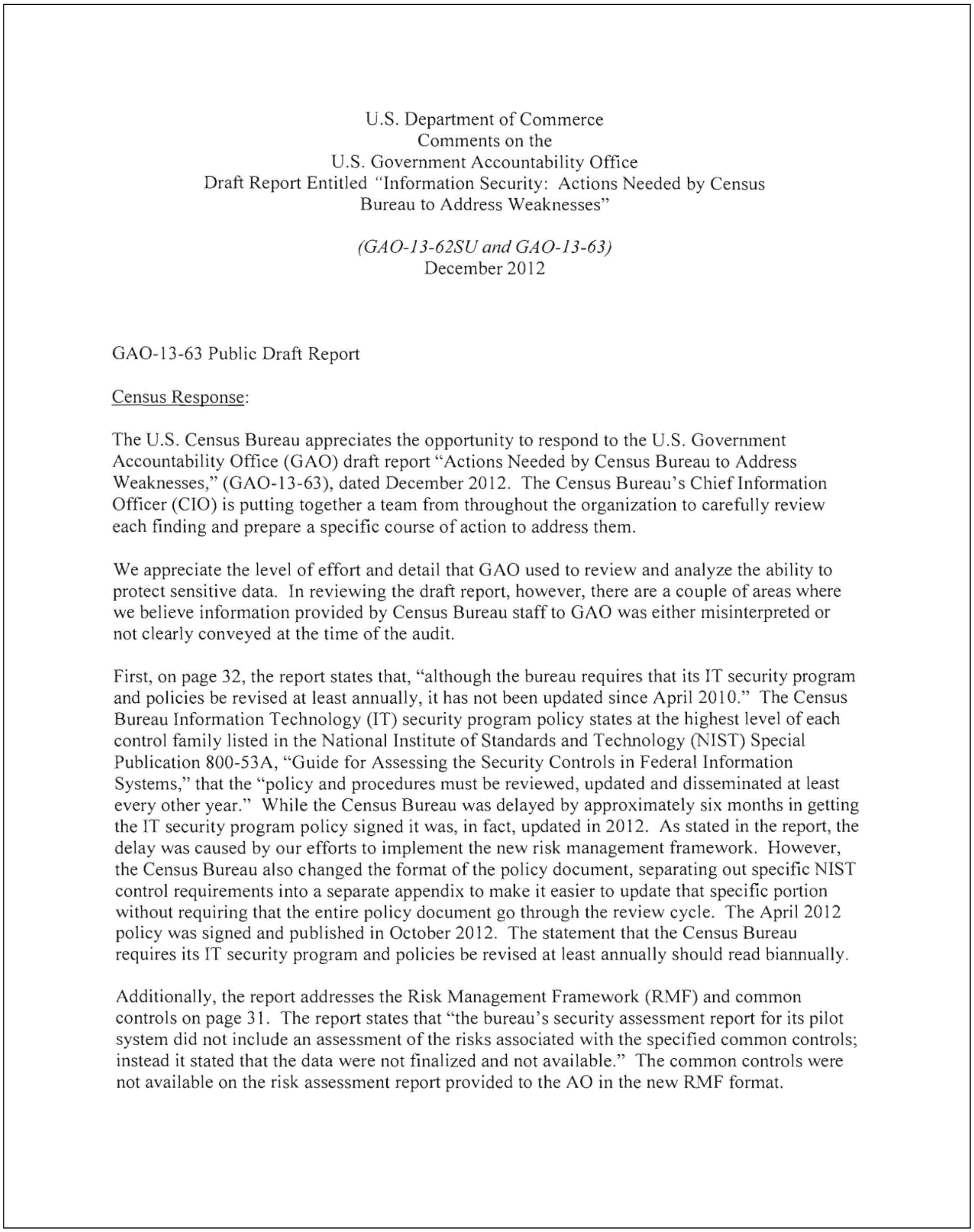
If you have any questions, please contact Jim Stowers, Deputy Assistant Secretary for Legislative and Intergovernmental Affairs, at (202) 482-3663.

Sincerely,

Rebecca Blank

Rebecca M. Blank
Acting Secretary of Commerce

Enclosure



U.S. Department of Commerce
Comments on the
U.S. Government Accountability Office
Draft Report Entitled "Information Security: Actions Needed by Census
Bureau to Address Weaknesses"

(GAO-13-62SU and GAO-13-63)
December 2012

GAO-13-63 Public Draft Report

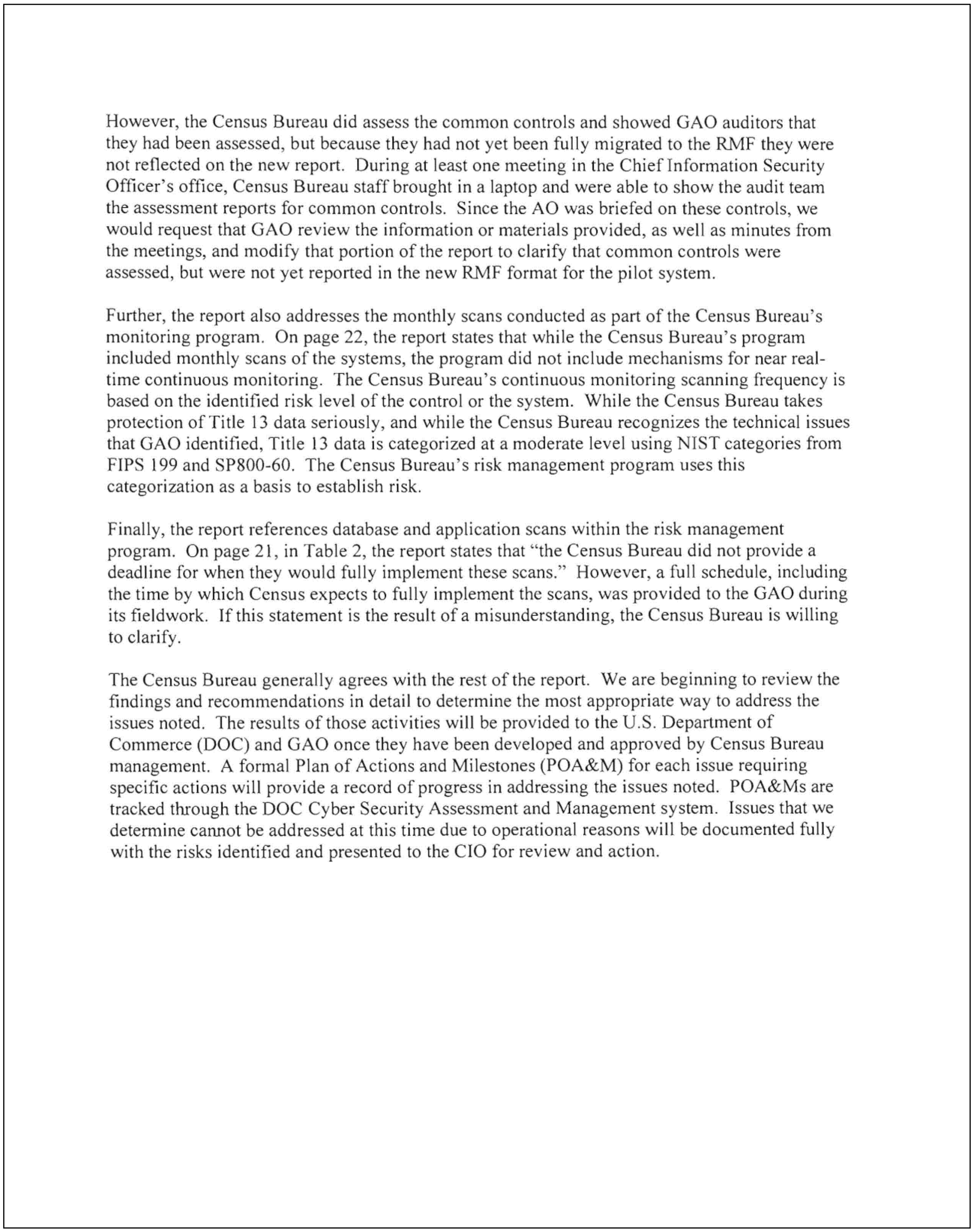
Census Response:

The U.S. Census Bureau appreciates the opportunity to respond to the U.S. Government Accountability Office (GAO) draft report "Actions Needed by Census Bureau to Address Weaknesses," (GAO-13-63), dated December 2012. The Census Bureau's Chief Information Officer (CIO) is putting together a team from throughout the organization to carefully review each finding and prepare a specific course of action to address them.

We appreciate the level of effort and detail that GAO used to review and analyze the ability to protect sensitive data. In reviewing the draft report, however, there are a couple of areas where we believe information provided by Census Bureau staff to GAO was either misinterpreted or not clearly conveyed at the time of the audit.

First, on page 32, the report states that, "although the bureau requires that its IT security program and policies be revised at least annually, it has not been updated since April 2010." The Census Bureau Information Technology (IT) security program policy states at the highest level of each control family listed in the National Institute of Standards and Technology (NIST) Special Publication 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems," that the "policy and procedures must be reviewed, updated and disseminated at least every other year." While the Census Bureau was delayed by approximately six months in getting the IT security program policy signed it was, in fact, updated in 2012. As stated in the report, the delay was caused by our efforts to implement the new risk management framework. However, the Census Bureau also changed the format of the policy document, separating out specific NIST control requirements into a separate appendix to make it easier to update that specific portion without requiring that the entire policy document go through the review cycle. The April 2012 policy was signed and published in October 2012. The statement that the Census Bureau requires its IT security program and policies be revised at least annually should read biannually.

Additionally, the report addresses the Risk Management Framework (RMF) and common controls on page 31. The report states that "the bureau's security assessment report for its pilot system did not include an assessment of the risks associated with the specified common controls; instead it stated that the data were not finalized and not available." The common controls were not available on the risk assessment report provided to the AO in the new RMF format.



However, the Census Bureau did assess the common controls and showed GAO auditors that they had been assessed, but because they had not yet been fully migrated to the RMF they were not reflected on the new report. During at least one meeting in the Chief Information Security Officer's office, Census Bureau staff brought in a laptop and were able to show the audit team the assessment reports for common controls. Since the AO was briefed on these controls, we would request that GAO review the information or materials provided, as well as minutes from the meetings, and modify that portion of the report to clarify that common controls were assessed, but were not yet reported in the new RMF format for the pilot system.

Further, the report also addresses the monthly scans conducted as part of the Census Bureau's monitoring program. On page 22, the report states that while the Census Bureau's program included monthly scans of the systems, the program did not include mechanisms for near real-time continuous monitoring. The Census Bureau's continuous monitoring scanning frequency is based on the identified risk level of the control or the system. While the Census Bureau takes protection of Title 13 data seriously, and while the Census Bureau recognizes the technical issues that GAO identified, Title 13 data is categorized at a moderate level using NIST categories from FIPS 199 and SP800-60. The Census Bureau's risk management program uses this categorization as a basis to establish risk.

Finally, the report references database and application scans within the risk management program. On page 21, in Table 2, the report states that "the Census Bureau did not provide a deadline for when they would fully implement these scans." However, a full schedule, including the time by which Census expects to fully implement the scans, was provided to the GAO during its fieldwork. If this statement is the result of a misunderstanding, the Census Bureau is willing to clarify.

The Census Bureau generally agrees with the rest of the report. We are beginning to review the findings and recommendations in detail to determine the most appropriate way to address the issues noted. The results of those activities will be provided to the U.S. Department of Commerce (DOC) and GAO once they have been developed and approved by Census Bureau management. A formal Plan of Actions and Milestones (POA&M) for each issue requiring specific actions will provide a record of progress in addressing the issues noted. POA&Ms are tracked through the DOC Cyber Security Assessment and Management system. Issues that we determine cannot be addressed at this time due to operational reasons will be documented fully with the risks identified and presented to the CIO for review and action.

Appendix III: GAO Contacts and Staff Acknowledgments

Contacts

Gregory C. Wilshusen, (202) 512-6244, wilshuseng@gao.gov
Dr. Nabajyoti Barkakati, (202) 512-4499, barkakatin@gao.gov

Staff Acknowledgments

In addition to the individuals named above, the following made key contributions to this report: Ed Alexander, West Coile, Vijay D’Souza, Duc Ngo, and Chris Warweg (assistant directors), Angela Bell, Saar Dagani, Nancy Glover, Thomas J. Johnson, Myong Kim, Vernetta Marquis, Justin Palk, John Spence, and Eugene Stevens.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Please Print on Recycled Paper.