

*U.S. DEPARTMENT OF COMMERCE*  
*Office of Inspector General*

---



*BUREAU OF THE CENSUS*

*Weaknesses in Census Bureau's Certification  
And Accreditation Process Leave Security of  
Critical Information Systems in Question*

*Final Inspection Report No. OSE-16519-1/August 2004*

**PUBLIC  
RELEASE**

*Office of Inspector General*

## CONTENTS

EXECUTIVE SUMMARY .....	i
INTRODUCTION .....	1
OBJECTIVES, SCOPE, AND METHODOLOGY .....	3
FINDINGS AND RECOMMENDATIONS.....	5
I. Certification and Accreditation Packages Were Significantly Deficient .....	5
A. Risk Assessments Did Not Provide an Adequate Basis for Identifying Security Requirements or Determining Whether Security Controls Are Sufficient.....	5
B. Sensitivity Assignments and Security Control Information in Security Plans Were Inappropriate and Inconsistent .....	5
C. Certification and Accreditation Decisions Were Based on Inadequate and Inconsistent Testing .....	7
D. One National-Critical System Had No Contingency Plan .....	9
E. Certification and Accreditation Memoranda Lacked Key Information .....	9
F. Conclusion.....	10
II. Designated Approving Authority for Accreditation Should Be Official with Management, Operational, and Budget Authority Over System.....	14
III. Plans of Action and Milestones Did Not Accurately Reflect System Security Deficiencies .....	15
IV. Additional Efforts Are Needed to Improve Specialized Security Training.....	16
V. A Patch Management Process Has Been Established.....	17
Attachment: Census Bureau's Response	

## EXECUTIVE SUMMARY

The Federal Information Security Management Act (FISMA)<sup>1</sup> requires agencies to review their information security program annually and Offices of Inspector General (OIGs) to conduct independent evaluations of those programs annually as well. Pursuant to FISMA, we evaluated the Census Bureau's information security program in terms of its compliance with the act as well as with Office of Management and Budget (OMB) requirements and the Department of Commerce's IT security policy.

Census's IT system definitions were changed significantly in FY 2003. According to the bureau, it reexamined its inventory of IT systems and determined that based on the overall mission, organizational structure, and responsibilities of individual directorates, the inventory structure was not reflective of operations. Census's IT Security Office therefore worked with contractors, system owners, and administrators to reorganize and consolidate the bureau's 87 systems. Grouping systems according to shared missions, ownership, and management yielded 11 program area systems, each having an associated set of component systems. Of the 11 program area systems, 2 are designated national critical (part of the critical infrastructure), 7 as mission critical, and 2 as business essential.<sup>2</sup> Each of the 11 systems and individual component systems has a security plan.

The purpose of our review was to evaluate (1) Census's IT Security Program Policies, issued in March 2003, (2) the impact of the IT systems consolidation on system security and the certification and accreditation process, (3) management and implementation of the plans of action and milestones (POA&M) process for program and system level weaknesses, (4) the bureau's plan to provide specialized IT security training to IT security officers and other staff having specialized IT security responsibilities, (5) the patch management process for correcting system security vulnerabilities, and (6) the bureau's incorporation of IT security into its capital planning and investment control process. Our focus was the security of Census's national-critical and mission-critical systems.

At the time of our fieldwork, capital asset plans for FY 2006 were in preparation and continuously changing. We were therefore unable to evaluate whether they adequately documented system security requirements and appropriately justified projected security expenditures. In addressing our remaining objectives, however, we found that Census's IT security program generally conformed in structure and intent with requirements of the Department's IT security program policy and other mandates, but that in practice it did not

---

<sup>1</sup> Title III, E-Government Act of 2002 (P.L. 107-347).

<sup>2</sup> The Critical Infrastructure Act of 2001, 42 U.S.C. 5195c, which is part of the USA Patriot Act of 2001 (P.L. 107-56) defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." According to OMB, an infrastructure or resource is considered mission critical if its damage or destruction would have a debilitating impact on the organization's ability to perform essential functions and activities. All other systems are considered business essential.

always appropriately apply those requirements, with the result that critical systems may not be adequately protected. Our specific findings are as follows.

**Certification and Accreditation Packages Were Significantly Deficient.** Certifying and accrediting information systems is a critical element of the bureau's IT security program. However, the certification and accreditation packages we reviewed did not comply with either Department or FISMA requirements in a number of areas: the documentation contained risk assessments that did not sufficiently identify system vulnerabilities and thus failed to serve as an adequate basis for identifying needed security controls; included security plans that assigned improper and inconsistent sensitivity levels to systems and did not adequately describe the controls that were in place or needed; and did not provide a contingency plan for one certified and accredited national-critical system. The packages also did not identify residual risks in the certified and accredited systems, and thus provided no evidence that the accrediting official understood the level of risk being assumed in authorizing system operations.

*Certification* is the formal testing of the security safeguards and controls implemented in a computer system to determine whether they meet applicable requirements and specifications.

*Accreditation* is management's formal authorization to allow systems to operate and it includes an explicit acceptance of the identified residual risks.

*System sensitivity* refers to FISMA's three security objectives for information and information systems: *confidentiality*, *integrity*, and *availability*. System owners must assign a sensitivity level of high, medium, or low to each objective to reflect the impact that a system's compromise would have on the agency's mission, and must justify the level assigned.

Further compromising IT system security was the bureau's decision to certify systems at levels below those necessary to ensure their adequate testing in order to meet the Department's December 2003 deadline for certification and accreditation of all national- and mission-critical systems. (See page 5.)

**Designated Approving Authority Should Be Official with Management, Operational, and Budget Authority Over System.** Departmental and OMB policy specify that designated approving authorities (DAAs) or accrediting officials must be program officials who have management, operational, and budget authority for the system, and that they may not be system owners—division or office chiefs. Census's policy, however, names its chief information officer (CIO) as the DAA for all systems, even though this official does not have the required authority over the bureau's entire inventory. (See page 13.)

**Plans of Action and Milestones (POA&Ms) Do Not Accurately Reflect System Security Deficiencies.** Contrary to OMB and the Department's security policy, Census is not using POA&Ms to list all identified security weakness and to track and manage efforts to resolve them. POA&Ms did not identify residual risks for which additional controls are needed, the lack of contingency plans, or the need for additional testing to ensure that systems are certified at a level commensurate with their sensitivity. (See page 14.)

**Additional Efforts Are Needed to Improve Specialized Security Training.** Department policy requires operating units to give specialized training to personnel who have significant IT security responsibilities and to track the status of efforts to provide such training. We found

limited progress in meeting these requirements at Census. While the bureau has identified positions for which specialized training is necessary, few of these staff have completed available security courses. Census is developing a capability to track training activity and expects to have this capability by the end of FY 2004. (See page 15.)

**A Patch Management Process Has Been Established.** As required by Department policy, Census has implemented a patch management process to identify, test, apply, and monitor the status of security patches<sup>3</sup> relevant to bureau systems. The process determines the need for patches and acquires, tests, applies, and monitors them on all information system components. (See page 16.)

We made numerous recommendations to Census for improving its certification and accreditation packages, ensuring POA&Ms document all known security weaknesses, and ensuring bureau personnel having IT security responsibility receive specialized training. Bureau officials have been receptive to our recommendations and have begun to take actions to implement many of them.

...

In its response to our draft report, Census stated that it generally agreed with our findings and described actions being taken or planned to address our recommendations. However, several of the actions do not adequately address the corresponding recommendation. The bureau needs to ensure that the residual risks of its IT systems are not accepted unless the remaining known vulnerabilities pose an acceptable level of risk to agency operations and assets, testing commensurate with the level of each system's sensitivity is performed, and POA&Ms contain all known information security weaknesses, including those identified through certification and accreditation. Following each recommendation, we have included a brief synopsis of the bureau's response and, where appropriate, our comments. The bureau's complete response is included as an attachment to this report.

---

<sup>3</sup> A patch is a piece of software code that is inserted into a program to fix a defect or eliminate a vulnerability.

## INTRODUCTION

The Federal Information Security Management Act (FISMA)<sup>1</sup> requires agencies to review their information security program annually and Offices of Inspector General (OIGs) to conduct independent evaluations of those programs annually as well. Pursuant to FISMA, we evaluated the Census Bureau's information security program, looking at its compliance with FISMA, Office of Management and Budget (OMB) requirements, and the Department of Commerce's IT security policy.

The Census Bureau's *IT Security Program Policies*, issued in March 2003, provides the requirements for its information security program. It specifies mandatory and recommended program management practices; security roles and responsibilities for bureau managers, employees, and contractors; and policies regarding management, operational, and technical controls. Aside from one exception (see finding II of this report), the bureau's policy is generally consistent with the Department of Commerce's IT security program policy.

The associate director for information technology and chief information officer (CIO) is responsible for implementing and overseeing the bureau's IT security program. The IT security officer heads the IT security office and reports to the CIO. The IT security officer is the bureau's IT security authority, serves as the central point of contact for the IT security program, and has authority for setting the program's day-to-day direction and overall goals, objectives, and priorities. System owners—division or office chiefs throughout the bureau—are responsible for complying with all IT security program policies and procedures and coordinating and implementing security controls for information systems under their control. System owners appoint division security officers to implement system-level security controls and maintain system documentation.

Certifying and accrediting information systems is a critical element of the bureau's IT security program. Certification is the formal testing of the security safeguards and controls implemented in a computer system to determine whether they meet applicable requirements and specifications. The system certifier, through the formal testing process, identifies residual risks—those risks that were not eliminated by implementation of security controls. Accreditation is management's formal authorization to allow systems to operate, and it includes an explicit acceptance of the identified residual risks. The accrediting official, known as the designated approving authority (DAA), relies on input from the certifier in determining whether to authorize system operation. The DAA may decide additional controls should be implemented to reduce or eliminate the residual risks, or may determine the residual risks are low and controls not cost-effective.

Department policy requires Commerce operating units to follow the National Security Agency's *National Information Assurance Certification and Accreditation Process* (NIACAP) for certifying and accrediting systems, but to document the process in a system security plan certification and accreditation package (as opposed to using NIACAP documentation guidelines). This package is to include a risk assessment, system security plan, contingency

---

<sup>1</sup> Title III, E-Government Act of 2002 (P.L. 107-347).

plan, certification test plan and test results, identification of residual risks, the certifier's recommendation, and an accreditation statement signed by the DAA indicating whether the system is authorized to operate and, if so, affirming that this official understands any related residual risks.

Further, the Office of Management and Budget (OMB) requires agencies to prepare plans of action and milestones (POA&Ms) that reflect all known IT security weaknesses within the agency and its components or bureaus. The agency, major components and program officials, and the IG are to use POA&Ms as the authoritative management mechanism to prioritize, track, and manage all agency efforts to close security gaps. POA&Ms thus provide the means for documenting security weaknesses identified during certification and other review processes.

### *IT Systems Redefined*

Census's IT system definitions were changed significantly in FY 2003. According to the bureau, it reexamined its inventory of IT systems and determined that based on the overall mission, organizational structure, and responsibilities of individual directorates, the inventory structure was not reflective of operations. Census's IT Security Office therefore worked with contractors, system owners, and administrators to reorganize and consolidate the bureau's 87 systems. Grouping systems according to shared missions, ownership, and management yielded 11 program area systems, each having an associated set of component systems. Of the 11 program area systems, 2 are designated national critical (part of the critical infrastructure), 7 as mission critical, and 2 as business essential.<sup>2</sup>

The bureau developed security plans for each of these 11 systems, as well as for the component systems. Each program area security plan is intended to document the management, operational, and technical controls that apply to associated component systems, whereas the security plans for the individual component systems are to describe controls specific to each component.

---

<sup>2</sup> The Critical Infrastructure Act of 2001, 42 U.S.C. 5195c, which is part of the USA Patriot Act of 2001 (P.L. 107-56) defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." According to OMB, an infrastructure or resource is considered mission critical if its damage or destruction would have a debilitating impact on the organization's ability to perform essential functions and activities. All other systems are considered business essential.

## OBJECTIVES, SCOPE, AND METHODOLOGY

The purpose of our review was to evaluate (1) Census's IT Security Program Policies, issued in March 2003, (2) the impact of the IT systems consolidation on system security and the certification and accreditation process, (3) management and implementation of the POA&M process for program and system level weaknesses, (4) the bureau's plan to provide specialized IT security training to IT security officers and other staff having specialized IT security responsibilities, (5) the patch management process for correcting system security vulnerabilities, and (6) the bureau's incorporation of IT security into its capital planning and investment control process.

A principal focus of our evaluation was a review of certification and accreditation materials. For the bureau's two national-critical IT systems, we evaluated complete certification and accreditation packages, which included system security plans, self-assessments, risk assessments, contingency planning information, results of vulnerability scans, and security test and evaluation materials. At the time of our fieldwork, the bureau was revising the certification and accreditation packages for its seven mission-critical systems; consequently, we were only able to evaluate the security plans for these systems, as the other materials were undergoing changes.

We used the following as criteria for assessing the bureau's security program:

- FISMA
- OMB Memorandum M-03-19, "Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting"
- National Security Telecommunications and Information Systems Security Instruction No. 1000, *National Information Assurance Certification and Accreditation Process (NIACAP)*
- OMB Circular A-130, Appendix III, "Security of Federal Automated Information Systems"
- NIST Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*
- NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*
- NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*
- NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*
- U.S. Department of Commerce, *IT Security Program Policy and Minimum Implementation Standards*
- U.S. Department of Commerce, System Security Plan Certification and Accreditation Package (SSPCAP) Requirements Inspection Checklist, version 2, June 30, 2003

In addition to reviewing certification and accreditation materials, we assessed the bureau's IT security policy and met with its CIO, IT security officer, and IT security staff. Because our findings on system consolidation contain sensitive information, we have presented them in a



separate draft report entitled, *The Census Bureau Should Redefine Its National-Critical Systems*, OSE-16519-2.

At the time of our fieldwork, the bureau was preparing capital asset plans for submission to the Department as part of the FY 2006 budget request. Because these plans were incomplete and continuously changing, we were unable to evaluate whether they contained adequate documentation for system security requirements and appropriate justification for projections of security expenditures.

We conducted our evaluation in accordance with the Quality Standards for Inspections issued by the President's Council on Integrity and Efficiency and under the authority of the Inspector General Act of 1978, as amended. We performed our fieldwork between November 2003 and April 2004.

## FINDINGS AND RECOMMENDATIONS

### I. Certification and Accreditation Packages Were Significantly Deficient

The certification and accreditation packages we reviewed had incomplete and inaccurate security plans and risk assessments, and one national-critical system was certified and accredited without having a contingency plan. The packages did not identify residual risks in the certified and accredited systems. Neither did they address whether the accrediting official understood the level of risk being assumed in authorizing system operations. Finally, the bureau's national-critical and mission-critical systems were certified and accredited without adequate testing.

#### A. *Risk Assessments Did Not Provide an Adequate Basis for Identifying Security Requirements or Determining Whether Security Controls Are Sufficient*

Department policy and NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, require agencies to identify system vulnerabilities, threats, and associated impacts so that appropriate and cost-effective controls can be established to mitigate related risks. The bureau's risk assessments for three of the four components of its national-critical systems were checklists on which the reviewer indicated whether or not listed security controls were implemented and/or applicable to the component. However, the assessments did not identify vulnerabilities, threats, impacts, and risks affecting the component systems. Thus, the risk assessments failed to serve as an adequate basis for determining whether the existing security controls were appropriate and whether additional controls were needed.

#### B. *Sensitivity Assignments and Security Control Information in Security Plans Were Inappropriate and Inconsistent*

FISMA defines three security objectives for information and information systems: *confidentiality*, *integrity*, and *availability*. System owners must assign a sensitivity level of high, medium, or low to each objective to reflect the impact that a system's compromise would have on the agency's mission, and must justify the level assigned. For example, the owner of a system that collects, processes, and distributes information subject to Title 13 and Title 26<sup>3</sup> restrictions might assign a sensitivity level of high to confidentiality and integrity, but medium to availability if system users can tolerate system outages lasting several days. Sensitivity assignments are used to establish the appropriate security controls needed to adequately protect the data. They also determine the rigor of testing and analysis required to certify and accredit a system.

#### *Improper and inconsistent sensitivity levels*

The sensitivity assignments in the security plans we reviewed were not always appropriate to the system or were inconsistent with the program area that a particular system supported. For example, the plan for an infrastructure system assigned sensitivity levels of medium for

---

<sup>3</sup> Titles 13 and 26 of the United States Code place restrictions on the disclosure of collected information.

confidentiality, medium for integrity, and high for availability. Yet the plans for systems that rely on this infrastructure system assigned sensitivity levels of high for all three objectives. If the infrastructure system is supporting systems that must be rigorously protected against unauthorized access, change, or damage and if it is relied upon by systems that must provide timely and reliable access to their information, the sensitivity levels for all three objectives of the infrastructure system must also be high. We discussed this discrepancy with bureau IT security staff, who agreed that the sensitivity levels for confidentiality, integrity, and availability for the infrastructure system should match those of the systems relying on it.

In addition, assigned sensitivity levels in security plans for some program area systems were not adequately supported, and in some instances the justification narrative actually supported the need for a higher level or did not match the system being described. For example, the justification for the infrastructure system's *medium* sensitivity level for confidentiality stated, "Data collected and stored in the Census Bureau's infrastructure systems contains demographic and economic information that, if disclosed to unauthorized sources, would cause a violation of Titles 26 and 13, U.S.C." This justification supports a sensitivity assignment of *high* for confidentiality. In another case, a justification incorrectly characterized a system's functions, noting that a medium level for availability was required to ensure currency of budget information and timeliness of financial reports, even though the system processes geography—not budget—data, and does not produce financial reports.

### **Inappropriate security controls**

The Department's policy and guidance state that security plans must describe the management, operational, and technical controls that are and will be implemented to meet system security requirements.

Bureau officials told us that security plans for program area systems are to document the management, operational, and technical controls that apply to *all* component systems, whereas the plans for component systems should describe controls specific to each component. However, the security plans we reviewed did not provide sufficient detail about security controls: the program area plans for the two national-critical systems did not describe planned or implemented controls either for themselves or their component systems. Instead, the plans described the purpose of each control and contained a copy of the bureau's security policy for that control.

Furthermore, security plans for some individual components of the national-critical systems did not provide accurate, complete, and detailed descriptions of controls that were implemented and planned. For example, one of the plans did not address any technical controls; another described identification and authentication controls that did not conform to the bureau's password policy.

In reviewing the program area system security plans for the seven mission-critical systems, we found that they, like their national-critical counterparts, did not describe controls but merely repeated portions of the bureau's security policy.

### ***C. Certification and Accreditation Decisions Were Based on Inadequate and Inconsistent Testing***

The Department CIO established a deadline of December 31, 2003, for certification and accreditation of all national-critical and mission-critical systems, and the bureau reported that it had met the deadline. However, we found that, in meeting the deadline, Census certified its systems at levels below those required to ensure they were adequately tested. NIACAP requires that systems be certified at one of four levels, with level 1 representing the least rigorous verification of security controls and level 4 representing the most rigorous. The certification level is dictated by the system's sensitivity level, which, as noted earlier, is determined by the criticality of the information processed and is used to establish the appropriate security controls needed to adequately protect the data. The increasing rigor of testing as system sensitivity increases is designed to give agencies greater assurance that systems with higher confidentiality, integrity, and availability requirements are protected and to help them avoid spending resources unnecessarily on lower risk systems.

The levels at which the bureau was planning to certify its critical systems—level 3 for its mission-critical infrastructure system and level 2 for its national-critical and remaining mission-critical systems—are not commensurate with the sensitivity of these systems. And in fact, in meeting the Department deadline, the bureau certified mission-critical systems—including infrastructure—at level 1, as the process at this level was more expedient. National-critical systems were certified at level 2, as planned.

The required testing at these levels was not rigorous enough to determine whether the systems' security controls provided the needed protection. Bureau officials told us that they planned to perform additional testing after the December deadline and increase certification levels accordingly. However, systems have not yet been tested at the appropriate level.

#### **Certification levels were not commensurate with system sensitivity**

Certification using NIACAP requires testing of system security controls, a process generally referred to as certification testing or security test and evaluation, to determine whether all required controls for ensuring confidentiality, integrity, and availability have been implemented and are performing as intended. The amount and type of testing is determined by the certification level (see table 1). Although the additional testing for level 4 is not defined, in our opinion it should include internal penetration testing.<sup>4</sup>

In determining the level at which to certify its systems, the bureau did not apply Department guidance appropriately and determined that both of its national-critical systems and six of its seven mission-critical systems should be certified at level 2, and the remaining mission-critical system (infrastructure) should be certified at level 3. Based on their sensitivity, however, all of

---

<sup>4</sup> An internal penetration test mimics an internal attack by a malicious employee/user and is intended to reveal weaknesses that allow for misappropriation of or damage to sensitive data.

these systems should be certified at a level 3 or 4. The lower levels mean that the systems would be certified with inadequate testing. The bureau's decision to certify all mission-critical systems at level 1 to meet the Department's deadline only made matters worse, as even less testing was required. Bureau officials stated that they intended to increase the certification level of six of these systems to level 2 and the infrastructure system to level 3 by December 31, 2004, and conduct the additional testing required. As discussed below, the additional testing Census planned and had conducted at the time of our fieldwork was not sufficient.

**Table 1. Required Testing by Level of Certification**

<b>Certification Level</b>	<b>Testing</b>
1	Checklist: using NIST SP 800-26, <i>Security Self-Assessment Guide for Information Technology Systems</i>
2	Abbreviated: Level 1 plus system vulnerability scanning
3	Moderate: Level 2 plus external penetration testing <sup>5</sup>
4	Extensive: more rigorous than Level 3

Further, we note that neither NIACAP nor Department policy endorses the incremental approach to certification the bureau was pursuing. Systems that are not tested at a level commensurate with their confidentiality, integrity, and availability requirements should not be considered certified and accredited, nor should they be reported as such.

**Certification testing was incomplete**

Census developed 267 tests, which map directly to its IT security policy, as the basis for certification testing. Each policy item that could be interpreted as a security requirement was assigned a unique number, and a test was developed to evaluate the effectiveness of its implementation. Because the bureau's policy covers the management, operational, and technical controls discussed in NIST's IT self-assessment guide, as required by Department policy, as well as other required controls,<sup>6</sup> this set of tests adequately supports level 1 certification testing. In

<sup>5</sup> An external penetration test mimics an attack by an external entity attempting to breach internal networks via the Internet.

<sup>6</sup> Including those in NIST guidance for developing IT system security plans.

addition, the bureau performs vulnerability scans on all systems and intends to conduct external penetration testing for its level 3 system.

In certifying its 2 national-critical systems, the bureau determined that 30 of its 267 tests were not applicable. It thus completed certification using the remaining 237 tests, as well as vulnerability scans. In certifying the 6 mission-critical systems at level 1, the bureau used only 130 of the 267 tests, reportedly to mitigate the considerable time and resources required to test the more than 80 component systems subsumed by the 6. But this subset of tests provides a much less exhaustive analysis of controls and, based on Department guidance, is not sufficient even for level 1 certification. Moreover, in increasing certification to level 2 for the 6 mission-critical systems, the bureau reported that it planned only to rescan these systems, but not apply the tests that had been omitted previously. To be adequately evaluated at level 2, all components of mission-critical systems must be subjected to all applicable tests from the full complement of 267, in addition to vulnerability scanning.

#### ***D. One National-Critical System Had No Contingency Plan***

Contingency plans are imperative: they establish the backup and recovery procedures for restoring a system's essential functions in the event of system loss or damage. Our review of the certification and accreditation package for one of Census's two national-critical systems found the following contingency planning deficiencies: (1) the contingency planning section of the program area security plan indicated that contingency information was included in an appendix, but the appendix did not exist; (2) there was no contingency plan for one of the system's two component systems, although a memorandum contained in the package stated that a plan was under development and would be completed and tested about 4 months after certification and accreditation; and (3) a plan for resuming business existed for the second component, but the package included a memorandum noting that a more robust plan would be developed and tested about 5 months following certification and accreditation.

Contingency plans should be prepared before systems are certified and accredited. At the very least, before certification was granted, the certifier should have noted the missing appendix and ensured that it was included and contained the required information. The certification and accreditation package should have identified the lack of contingency plans as a residual risk needing correction.

#### ***E. Certification and Accreditation Memoranda Lacked Key Information***

Department guidance issued in June 2003 specifies that each system certification and accreditation package must include a memorandum, signed by the system certifier, that summarizes and affirms the results of the certification tests; identifies residual risks; and recommends specific corrective actions as warranted as well as whether accreditation should be granted in full, for an interim period, or denied. The package also is to include an accreditation statement signed by the DAA stating (1) what accreditation action was taken and (2) that the DAA understands and accepts any residual risks of operating the system. This statement may

also direct the system owner to take action to further mitigate risk and to track such actions in a POA&M.

The certification and accreditation packages for both of the bureau's national-critical systems included a memorandum signed by the certifier, the DAA, a bureau program manager, and two user representatives. However, the signing DAA was the CIO, which, as noted in finding II, is inappropriate because the CIO does not have management, operational, and budget authority for these systems. Moreover, neither memorandum identifies residual risks and associated corrective actions or includes an accreditation recommendation. Nor do the packages contain an accreditation statement. In fact, residual risks were not identified anywhere in the package. Without an explicit identification of risks, it is unclear how the test results were interpreted by the certifier, what particular risks the DAA agreed to assume, and whether the accrediting official fully understood the risks being accepted. The bureau's IT security officer indicated that in the accreditation briefing for these systems presented to the CIO, residual risks were discussed, but acknowledged that they had not been formally documented in the memoranda, elsewhere in the package, or on system POA&Ms.

#### ***F. Conclusion***

We discussed the problems we had identified in each system's certification and accreditation materials with bureau IT security officials, who generally agreed with our findings. They acknowledged the weaknesses with their risk assessments and are developing a new policy based on NIST risk assessment guidance. They indicated that a draft policy and associated risk assessment templates are nearing completion and that training on using the templates will be provided. Census needs to review the risk assessments for all program area and component systems after they are revised to ensure they contain complete and accurate information for determining system security controls.

The problems we identified with sensitivity assignments and lack of documented security controls are significant and should have been identified in the certification and accreditation process. Once identified, the appropriate sensitivity and controls should have been determined, and the systems reviewed to ascertain whether the required controls were implemented and working as intended. Because we found serious problems in some of the bureau's most critical systems, we are concerned that other sensitive systems may have similar shortcomings; they therefore need to be reviewed. If new security requirements and the need for additional security controls are identified as the risk assessments are revised and sensitivity levels reviewed, Census needs to ensure that appropriate security controls are implemented on the applicable systems and documented in security plans.

We advised Census that systems having high sensitivity levels for confidentiality, integrity, and availability should be certified at a level no less than 3, and require more extensive testing of security controls. Bureau officials told us the incremental certification and accreditation approach would be abandoned, the two national-critical systems and six of the mission-critical systems would be certified at level 3, the mission-critical infrastructure system would be certified at level 4, and appropriate testing would be performed. However, as of June 2004, the two

national-critical systems and six mission-critical systems had been certified at level 2 rather than level 3 and the mission-critical infrastructure system at level 3 rather than level 4. The bureau did, however, use all 267 tests for these certifications.

Level 2 does not provide sufficient testing for mission-critical or national-critical systems. Mission-critical systems should be certified at level 3 or 4 depending on their sensitivity. Our draft report on the bureau's definition of its national-critical systems discusses the requirements for their use in a national security emergency and recommends that they be certified at level 4.<sup>7</sup>

### **Recommendations**

The director of the Census Bureau should ensure that:

1. A new risk assessment policy based on NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, is developed and appropriate training provided.

**Synopsis of Census's Response:** The response states that the bureau's IT security office has issued a policy memorandum concerning the requirement to use NIST 800-30 as a guideline for preparing risk assessments and that a subsequent memorandum was issued by the CIO to reiterate the requirement. The IT security officer conducted formal training for all security officers and is working with program personnel to ensure they understand the requirements for risk management.

2. Risk assessments are revised using the new risk assessment methodology.

**Synopsis of Census's Response:** All risk assessments are being revised and the responsible official is acknowledging and accepting in writing any residual risks noted in the assessment. This information will be included in certification and accreditation documentation and presented to the system owner and DAA. This action is to be completed by September 30, 2004.

**OIG Comment:** Census officials should not accept residual risks unless the remaining known vulnerabilities pose an acceptable level of risk to agency operations and assets.

3. Specified sensitivity levels for confidentiality, integrity, and availability are appropriate, accurately justified, and consistent across all systems by having
  - a. system owners review the sensitivity levels specified in their program area security plans and revise them as necessary; and
  - b. the bureau's IT security officer review the sensitivity levels in all security plans to ensure they are appropriate and consistent across all systems.

---

<sup>7</sup> *The Census Bureau Should Redefine Its National-Critical Systems*, Draft Inspection Report No. OSE-16519-2, July 2004.



**Synopsis of Census's Response:** System owners and the IT security staff have reviewed the sensitivity levels in all security plans to ensure they are appropriate and consistent.

4. All program area and component system security plans are reviewed and revised as needed to provide detailed descriptions of security controls that are in place and planned.

**Synopsis of Census's Response:** System owners and IT security staff are reviewing the security plans to ensure that they present a sufficiently detailed description of the security controls in place or planned.

5. Any needed changes to a system's security controls identified in revised risk assessments and security plans are implemented as soon as possible.

**Synopsis of Census's Response:** After the risk assessments and security plans are updated and required changes to security controls identified, the IT security office will track their implementation using Plans of Action and Milestones (POA&M).

6. System certification and accreditation packages include
  - a. a memorandum signed by the certifier summarizing and affirming the results of certification tests, identifying residual risk not mitigated by adequate controls, recommending specific corrective actions as warranted, and advising whether the accrediting official should grant either full or interim accreditation, or should deny accreditation; and
  - b. an accreditation statement signed by the DAA stating, among other things, whether full or interim accreditation was granted, or whether it was denied, and that the DAA understands and accepts any residual risk of operating the system if processing is authorized.

**Synopsis of Census's Response:** The certification and accreditation of all critical systems were completed by May 19, 2004.

**OIG Comment:** This response does not indicate whether certification and accreditation of critical systems was completed in accordance with this recommendation. The bureau should ensure that certification and accreditation packages include the specified elements.

7. By December 31, 2004, all mission-critical systems are certified and accredited at the appropriate level—either level 3 or 4—depending on their sensitivity.

**Synopsis of Census's Response:** The bureau is developing a process for internal penetration testing of its mission-critical systems that will not interfere with critical processing schedules and is attempting to complete testing by the target date.

**OIG Comment:** The bureau's response refers only to internal penetration testing, which is needed for certifying level 4 systems, but does not address external penetration testing, which is needed for certifying both level 3 and level 4 systems. The bureau should ensure that appropriate testing is performed.

8. Contingency planning information in all program area and component system security plans is reviewed and revised to ensure its accuracy, and newly developed contingency plans are included in the certification and accreditation package for the system.

**Synopsis of Census's Response:** The IT security office is working with the program areas to ensure that contingency plans are accurate and complete, and is conducting joint reviews with staff managing the bureau's continuity of operations planning. Revised plans will be included in certification and accreditation packages.

## II. Designated Approving Authority for Accreditation Should Be Official with Management, Operational, and Budget Authority Over System

OMB Circular A-130 and the Department's policy both specify that designated approving authorities must be program officials who have management, operational, and budget authority for the system, and that DAAs may not be system owners. Census's policy is at odds with these requirements on two fronts. First, it names its CIO as the approving authority for all systems. However, the CIO does not have management, operational, and budget authority for the bureau's entire inventory of systems, and should therefore be DAA for only those over which he has such authority (e.g., technology infrastructure). Second, the bureau's policy allows the CIO or the Census Bureau director to make the system owner the DAA. During our fieldwork, we informed the bureau's IT security officer of these policy discrepancies, and he agreed to update the policy to conform to that of the Department.

Because bureau systems are tied to its technology infrastructure, the bureau's CIO has issued a memorandum stating that, for all but the infrastructure system, he will sign the accreditation memorandum to indicate his understanding of the system's status, any residual risk, and specific information relating to its certification and accreditation. The rationale is that the CIO is responsible for the technology infrastructure, and vulnerabilities in any connected system would leave the entire network vulnerable. The CIO's memorandum also identifies by name the bureau program official having management, operational, and budget authority for each system as its DAA. Because this role will likely be a new one for these officials, they will need information and training to ensure they fully understand their responsibilities. This is consistent with the recent memorandum from the Secretary of Commerce emphasizing the need for continued high priority for IT security, including sufficient training for accrediting officials.<sup>8</sup>

### Recommendations

The director of the Census Bureau should ensure that:

1. The bureau's information security policy is revised to require the DAA to be a program official with management, operational, and budget authority for the system being accredited.

**Synopsis of Census's Response:** The bureau will assign the DAA role to program officials with management, operational, and budget authority for the system being accredited. The Census Bureau CIO will countersign the authorization.

2. Program officials who will assume the role of DAA fully understand their new responsibilities and are adequately trained.

**Synopsis of Census's Response:** The IT security officer has issued written guidance to DAAs on their roles and responsibilities, and with assistance from the Human Resources Division, is developing methods to provide formal training.

---

<sup>8</sup> Memorandum from the Secretary of Commerce to Secretarial Officers and Heads of Operating Units, "Continued High Priority of IT Security," June 29, 2004.

### **III. Plans of Action and Milestones Did Not Accurately Reflect System Security Deficiencies**

Both OMB and the Department's security policy require that POA&Ms reflect all known IT security weaknesses and that agencies use these documents as their authoritative management mechanism to prioritize, track, and manage all efforts to close security gaps. The POA&Ms we reviewed did not list any of the weaknesses identified by the bureau during the certification and accreditation process. For example, although Census officials recognized weaknesses in their risk assessment approach and indicated they planned to improve it, these weaknesses were not recorded on a POA&M. POA&Ms also did not identify residual risks for which additional controls are needed, the lack of contingency plans for components of a certified and accredited system, or the need for additional testing to ensure that systems are certified at a level commensurate with their sensitivity. The lack of documented management, operational, and technical controls in the security plans and any associated system deficiencies should have been identified, as discussed in finding II, and included on the POA&Ms.

#### **Recommendation**

The director of the Census Bureau should take the necessary actions to ensure that POA&Ms appropriately document all known information security weaknesses and track corrective actions to closure.

**Synopsis of Census's Response:** The POA&M process has modified, and the IT security officer has begun notifying system owners and DAAs of the status of published weaknesses of their systems and the status of the corrective actions through monthly reports.

**OIG Comment:** It is unclear whether the modification to the POA&M process discussed in this response will ensure that all known security weaknesses are included on POA&Ms. POA&Ms must contain all known security weaknesses, including those identified in the certification and accreditation process.

#### **IV. Additional Efforts Are Needed to Improve Specialized Security Training**

Department policy requires operating units to provide specialized training for personnel having significant IT security responsibilities and to track progress made toward providing the training. We reported in last year's independent evaluation that training for personnel with significant information security responsibilities appeared to be inconsistent and incomplete at Census and the other units we reviewed.

In our current review of the Census Bureau, we found that some progress has been made toward providing specialized training. The bureau's security policy provides a list of staff positions that might require specialized security training and allows the IT security officer the discretion to expand the list.

In order to provide a more consistent approach to specialized IT security training, the Department has acquired an enterprise license for a web-based information security training program that offers specialized training courses in accordance with NIST 800-16 guidance and has made the program available to its operating units. The bureau's IT security officer has worked with security officers in its various divisions to identify courses that are appropriate for IT system security officers, system administrators, database administrators, DAAs, and other personnel who have security responsibilities.

The IT Security Office maintains a database that tracks specialized training taken by employees via the program, and is developing reports to identify (1) who received specialized training, (2) what the specialized training consisted of, and (3) when employees actually took the classes. Census plans to have the reporting capability in place by the end of FY 2004. Though such reports are not yet available, the IT security officer reports that only a small percentage of system and database administrators have completed courses related to their responsibilities. The bureau needs to make this training a priority and ensure that all personnel in need of specialized IT security training complete the courses relevant to their positions in a timely manner.

#### **Recommendations**

The director of the Census Bureau should ensure that:

1. Bureau personnel having IT security responsibility complete specialized security training related to their responsibilities.

**Synopsis of Census's Response:** The IT security office is working with the Human Resources Division to identify personnel with significant security responsibilities, who will then be notified of their training requirement. Computer-based training will be available.

2. Reports for tracking specialized training are developed and available for management review by the end of FY 2004.

**Synopsis of Census's Response:** The bureau has acquired a system to accomplish this.

## V. A Patch Management Process Has Been Established

Department policy requires each operating unit to have a process for identifying, tracking, and reporting on security patch management. Census has implemented a patch management process to identify, test, apply, and monitor the status of security patches relevant to bureau systems. The process determines the need for patches and acquires, tests, applies, and monitors patches to its information system components.

Patch management is initiated by both the bureau's computer incident response team (CIRT) and members of the IT

Security Office. Based primarily on alerts received from the Department's CIRT and the Federal Computer Incident Response Center (FedCIRC),<sup>9</sup> the bureau's CIRT sends an e-mail alert documenting necessary corrective actions to the local area network configuration management team (LAN CMT), which tracks whether appropriate action is taken and sends an e-mail confirmation to the bureau's CIRT. The IT Security Office validates whether appropriate corrective actions have been taken by performing vulnerability scans for specific alerts on affected systems.

In addition, members of the IT Security Office subscribe to various vendor notification lists and, upon learning of available security patches, e-mail the LAN CMT, which ensures that appropriate system administrators are notified to install the applicable patches. The bureau indicated that about 75 percent of all patches are tested before being applied to production systems and that patches associated with high criticality alerts are likely to be applied without testing.

Census uses commercial software products to maintain a current inventory of workstations, servers, and network devices. The products also identify the operating system and application software installed on them as well as applicable vulnerabilities, and distribute appropriate patches. The IT Security Office uses network scanners to confirm that patches for known vulnerabilities have been applied.

While we confirmed that the bureau has implemented a process to address this important area, time and resource constraints prevented us from confirming its effectiveness, and we have no recommendations for this finding.

A patch is a piece of software code that is inserted into a program to fix a defect. Patches are developed and released by software vendors when vulnerabilities are discovered. Patch management is critical to protecting computer systems from malicious attacks, and includes acquiring, testing, applying, and monitoring patches to a computer system. The CERT Coordination Center\* points out that about 95 percent of all network intrusions could be avoided by keeping systems up to date with appropriate patches. Thus it is important that agencies have in place effective patch management policy and procedures.

(\*The CERT Coordination Center is a repository of Internet security expertise located at the Software Engineering Institute, a federally funded research and development organization operated by Carnegie Mellon University.)

<sup>9</sup> FedCIRC is the federal civilian agencies' focal point for computer security incident reporting, prevention, and response. It is located in the Department of Homeland Security.




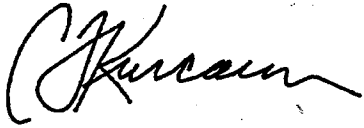
Attachment

**UNITED STATES DEPARTMENT OF COMMERCE**  
**Economics and Statistics Administration**  
**U.S. Census Bureau**  
Washington, DC 20233-0001  
OFFICE OF THE DIRECTOR

AUG 20 2004

MEMORANDUM FOR Judith J. Gordon  
Assistant Inspector General for  
Systems Evaluation

Through: Kathleen B. Cooper   
Under Secretary for Economic Affairs

From: Charles Louis Kincannon   
Director

Subject: *Weaknesses in Census Bureau's Certification and Accreditation  
Process Leave Security of Critical Information Systems in  
Question, Draft Inspection Report No. OSE-16519-1*

This is in response to your memorandum of July 23, 2004, requesting comments on the above-mentioned draft report. We generally agree with the report findings and address the recommendations as follows:

**Recommendations**

1. A new risk assessment policy (NIST SP 800-30) is developed and appropriate training provided.

**Census Bureau Response:** Action has already been taken on this recommendation. The Census Bureau's Information Technology (IT) Security Office issued a policy memorandum concerning the requirement to use NIST 800-30 as a guideline for preparing risk assessments. The IT Security Officer conducted formal training for all Division Security Officers (DSOs) and IT System Security Officers (ITSSOs) on July 20, 2004. Copies of the presentation were made available to all personnel on the IT Security Office Web site for reference, and the training session was videotaped and is available for reference on the Census Bureau's IP TV network. In addition, a formal memorandum was issued by the Census Bureau's Chief Information Officer (CIO) to all Division and Office Chiefs to reiterate the new requirements for risk assessments to be completed in accordance with NIST SP 800-30. The IT Security Office is continuing to work with program areas that have questions to ensure they understand the requirements for risk management.

USCENSUSBUREAU

Helping You Make Informed Decisions

www.census.gov

2. Risk assessments are revised using the new methodology.

**Census Bureau Response:** Currently, all program areas within the Census Bureau are revising their risk assessments under the guidelines of NIST SP 800-30. All risk assessments are being revised, and the responsible Division or Office Chief is acknowledging and accepting, in writing, any residual risks noted in the assessment. These documents are included in the certification and accreditation documentation for each component and presented to the system owner and Designated Accrediting Authority (DAA) of the system. Final drafts of the revised risk assessments are due to be completed by September 30, 2004.

3. Specified sensitivity levels for confidentiality, integrity, and availability are appropriate, accurately justified, and consistent across all systems by having
  - a. System owners review the sensitivity levels specified in their program area security plans and revise them as necessary; and
  - b. The Bureau's IT security officer review the sensitivity levels in all security plans to ensure they are appropriate and consistent across all systems.

**Census Bureau Response:** System owners have reviewed the sensitivity levels of the security plans they are responsible for, and revisions have been completed where necessary. The IT Security Officer and the staff of the IT Security Office have reviewed the sensitivity levels in all security plans to ensure that they are appropriate and consistent.

4. All program area and component system security plans are reviewed and revised as needed to provide detailed descriptions of security controls that are in place and planned.

**Census Bureau Response:** System owners and their DSO/ITSSOs are currently reviewing their security plans, along with the staff of the IT Security Office, to ensure that a more detailed description of the security controls in place or planned are adequate.

5. Any needed changes to a system's security controls are identified in revised risk assessments and security plans and are implemented as soon as possible.

**Census Bureau Response:** This recommendation will be addressed once the revised risk assessments and security plans are updated. The IT Security Office will review and track required changes to security controls identified through the Census Bureau Plan of Actions and Milestones (POA&M) process once the required changes are identified.