U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

U.S. Census Bureau

FY 2009 FISMA Assessment of the Field Data Collection Automation System (CEN22)

Final Report No. OAE-19728
November 2009

Office of Audit and Evaluation

UNITED STATES DEPARTMENT OF COMMERCE
Office of Inspector General
Washington, D.C. 20230

November 20, 2009

MEMORANDUM FOR: Dr. Robert M. Groves
Director
U.S. Census Bureau

Thomas L. Mesenbourg Jr.
Deputy Director and Chief Operating Officer
U.S. Census Bureau

FROM: Allen Crawley
Assistant Inspector General for Systems Acquisition and IT Security

SUBJECT: U.S. Census Bureau
FY 2009 FISMA Assessment of the Field Data Collection Automation System (CEN22)
Final Report No. OAE-19728

This is our report on the results of our Federal Information Security Management Act (FISMA) review of the bureau's certification and accreditation of the Field Data Collection Automation (FDCA) system.

We found that the authorizing official incorrectly determined that the risks identified by the certification agent were low at the time the authorization to operate was granted. Given that FDCA is mission critical and was needed to support decennial field operations that could not be delayed, the authorizing official should have extended the April 17, 2009, interim authorization to operate, rather than granting a full authorization. This would have allowed the system to operate under specific terms and conditions, while acknowledging greater risk to the agency for a specified period of time. We recognize the critical need for FDCA to continue to operate and provide support to decennial census operations, and thus have made recommendations to provide increased assurance that the system and its information will be adequately protected for the duration of the decennial census.

At the time the system was authorized, progress in correcting numerous and significant vulnerabilities was minimal. The certification agent noted that security features providing

layers of security redundancy could compensate for numerous vulnerabilities; however, our assessment of the compensating security features determined they were in fact not effectively protecting the system.

Our review also found that FDCA's system security plans and security control assessments were generally adequate, but need improvement. We also found that the bureau has not established, implemented, and assessed secure configuration settings for all IT products that are part of FDCA.

In its response to our draft report, Census concurred with all our findings and all but one of our recommendations; however, we find Census' planned action to address this recommendation is reasonable and responsive. Census's response is summarized in the appropriate sections of the report and is included in its entirety as appendix A.

We request that you provide us, within 60 calendar days of the date of this report, with an action plan describing the actions you have taken or plan to take in response to our recommendations. As required by FISMA, a plan of action and milestones should be used to communicate the plan.

We appreciate the cooperation and courtesies extended to us by your staff during our evaluation. If you would like to discuss any of the issues raised in this report, please call me at (202) 482-1855.

Attachment

cc: Suzanne Hilding, Chief Information Officer, U.S. Department of Commerce
Arnold A. Jackson, associate director for decennial census, U.S. Census Bureau
Brian E McGrath, associate director for information technology and chief information officer, U.S. Census Bureau
Patricia McGuire, program manager for field data collection automation program management office, U.S. Census Bureau
Timothy P. Ruland, chief, information technology office, U.S. Census Bureau
Adam C. Miller, Census audit liaison

Report In Brief

U.S. Department of Commerce, Office of Inspector General

November 2009

U.S. Census Bureau

FY 2009 FISMA Assessment of the Field Data Collection Automation System (OAE-19728)

Why We Did This Review

The Federal Information Security Management Act of 2002 (FISMA) requires federal agencies to identify and provide security protection of information collected or maintained by it or on its behalf. Inspectors general are required to annually evaluate agencies' information security programs and practices. Such evaluations must include testing of a representative subset of systems and an assessment, based on that testing, of the entity's compliance with FISMA and applicable requirements.

This review covers our evaluation of the Census Bureau's FDCA system, which is one of a sample of systems we assesed in FY 2009.

Background

FDCA is a contractor-designed system used by Census field workers to collect, process, and secure information for the decennial census. The FDCA system provides essential IT support for census field operations.

C&A is a process by which security controls for IT systems are assessed to determine their overall effectiveness. Understanding the remaining vulnerabilities identified during the assessment is essential in determining the risk to the organization's operations and assets, to individuals, to other organizations, and to the nation resulting from the use of the system.

What We Found

We evaluated certification and accreditation activities for the Field Data Collection Automation (FDCA) system as part of our FY 2009 reporting responsibilities under the Federal Information Security Management Act (FISMA).

On April 17, 2009, FDCA was granted an interim authorization to operate, allowing the system to operate under specific terms and conditions while vulnerabilities were assessed and corrected. On June 17, 2009, the authorizing official granted full operation of FDCA, even though at the time Census had made only minimal progress in correcting system weaknesses. We found that the authorizing official should have extended the interim authorization to operate rather than issuing a full authorization.

Our review also found that FDCA's system security plans and security control assessments were generally adequate, but need improvement. The bureau has not established, implemented, and assessed secure configuration settings for all IT products that are part of FDCA.

What We Recommend

We recognize the need for FDCA to continue to operate and provide support to decennial census operations, so our recommendations are intended to provide increased assurance that the system and its information will be adequately protected for the duration of the decennial census.

Census agreed with our findings and all but one of our recommendations. It partially concurred with this recommendation and described a reasonable and responsive alternative corrective action.

Listing of Abbreviated Terms and Acronyms

C&A	certification and accreditation
CIS	Center for Internet Security
CM	configuration management
DBMS	database management system
[redacted]	[redacted]
DPC	data processing center
FDCA	Field Data Collection Automation
FISMA	Federal Information Security Management Act of 2002
FOS	field operation supervisors
HHC	hand-held computers
[redacted]	[redacted]
IT	information technology
LCO	Local Census Office
NIST SP	National Institute of Standards and Technology Special Publication
OIG	Office of Inspector General
POA&M	plan of action and milestones
SA	system administrator
SAR	security assessment report
[redacted]	[redacted]
SSP	system security plan
[redacted]	[redacted]

Synopsis of Findings

- System security plans were generally adequate, but some minor improvements are needed.
- Census has not established, implemented, and assessed secure configuration settings for all IT products.
- Security control assessments were generally adequate, but improvements are needed.
- OIG control assessment found vulnerabilities requiring remediation.
- Overstatement of compensating security features and downplaying numerous vulnerabilities led to an ill-advised and inappropriate authorization decision.

Conclusion

We concluded that the decisions to recommend and grant an authorization to operate were inappropriate. But given the field data collection automation (FDCA) system's requirement to support decennial field operations on a fixed schedule, the authorizing official should have extended the April 17, 2009, interim authorization to operate.

The certification agent's recommendation to grant an authorization to operate was flawed because the progress in correcting numerous and significant vulnerabilities. In general, the certification agent did comprehensively assess security controls and identify numerous high-risk vulnerabilities. [redacted] The agent noted that security features providing layers of security redundancy could compensate for numerous vulnerabilities; however, our assessment of the compensating security features determined they were in fact not effectively protecting the system. The agent cited mission criticality as a factor in the recommendation. However, National Institute of Standards and Technology Special Publication (NIST SP 800-37) states that if the authorizing official deems that the risk is unacceptable, but there is an overarching mission necessity to place the information system into operation, an *interim* authorization to operate may be issued. An interim authorization provides a limited authorization to operate the information system under specific terms and conditions and acknowledges greater risk to the agency for a specified period of time.

The authorizing official incorrectly determined that the risks identified by the certification agent were low, and inappropriately granted the authorization to operate. Information concerning the high-risk vulnerabilities identified during the certification assessment, the compensating security features, and the progress made on remediating vulnerabilities were provided to the authorizing official. At the exit conference, the authorization official indicated he believed the decision to grant the June 17, 2009, authorization to operate was his only option to allow FDCA to remain in operation. However, as discussed previously, the interim authorization should have been extended.

Summary of Census Response

In its response to our draft report, Census concurred with all of our findings and all but one of our recommendations. It partially concurred with this recommendation and described alternative corrective action. Census also identified actions it will take to address our other findings and recommendations.

OIG Comments

After reviewing Census's planned action to address the recommendation it partially concurred with, we conclude that it is reasonable and responsive to the recommendation.

We address specific elements of Census's response in the applicable sections of the report and include the full response as appendix A.

Introduction

The FDCA system provides essential IT support for census field operations. The bureau is using this contractor-developed system to collect, process, and secure information for the decennial census.

Census has categorized FDCA as a [redacted] system, which means that a security breach could have a [redacted] effect on organizational operations, organizational assets, or individuals.

The OIG previously evaluated the FY 2008 dress rehearsal certification and May 30, 2007, accreditation of this system. In a report issued September 29, 2008, we concluded that:

- Census needed to improve security control assessments to assure that controls are implemented correctly, operating as intended, and meeting the security requirements for the system; and
- the authorizing official had not been provided the necessary information to make a credible, risk-based accreditation decision.

To meet the FY 2009 Federal Information Security Management Act (FISMA) reporting requirements, we evaluated the Census Bureau certification and accreditation (C&A) for the FDCA system (CEN22). For a complete outline of our objectives, scope, and methodology, see appendix B. FDCA is a critical system supporting the decennial address canvassing field operation. This evaluation addresses FDCA's C&A completed on June 17, 2009.

Certification & Accreditation Timeline

From May 2007 to June 2009, FDCA underwent a phased C&A process to permit operating the portions of the system necessary to prepare for and conduct decennial census activities, even though the development of the full FDCA system was incomplete. The list below provides a chronology of C&A activities during this time period.

- May 30, 2007 – Authorization to operate granted to support decennial census dress rehearsal.
- January 2, 2008 – Authorization to operate granted to include the operation of a new data processing center 2 (DPC2) until September 30, 2009.
- As a result of changing scope of the FDCA contract, many architectural changes mandated by Census, and the addition of new functionality, it became necessary to recertify and reaccredit the **entire** system.
- October 9, 2008 – Authorization to operate granted until January 2009 to continue system development and move into the production phase for address canvassing activities. DPC2 was not included in this authorization.
    - Certification assessments were incomplete.
    - Fifty-seven vulnerabilities were recorded on the system plan of action and milestones (POA&M).
- February 20, 2009 – Certification assessments were reported as completed.
- April 3, 2009 – Authorization granted to operate DPC2 until April 17, 2009, to support address canvassing begun on March 30, 2009.

  - The certification status and recommendation memo acknowledges that certification assessments reported as complete on February 20, 2009, actually have **not** been completed and are still underway. Incomplete assessments include DPC2 components.

- April 17, 2009 – Interim authorization to operate granted until June 17, 2009, for continuation of address canvassing activities.
  - Although certification tests are completed, the Information Technology Security Office is still assessing the information obtained from testing.

- April 22, 2009 – Certification status memo explains that certification assessments have been completed.
  - Approximately 1,100 vulnerabilities are acknowledged; this number is considered "very high" by the certification agent.
  - An approval to operate (non-interim) will not be granted until the vulnerabilities and the lack of sound documentation have been addressed.

- June 17, 2009 – Authorization to operate all aspects of the FDCA system is granted.
  - The authorizing official explains that residual risks to the system are low.
  - Authorization will expire June 17, 2012.

Findings and Recommendations

1. System Security Plans Were Generally Adequate, but Some Minor

- The initial security plan was approved at the conclusion of the C&A initiation phase on January 13, 2008. The plan was updated June 5, 2009, and provided to the authorizing official. Both plans were generally adequate. Our evaluation found that both plans include
  - system descriptions that provide a clear overview of the system architecture and functionality;
  - applicable security control enhancements and organization-defined parameters necessary for tailoring security controls;
  - adequate descriptions of planned portions of security controls; and
  - descriptions of how security controls are implemented across the diverse components included in the system accreditation boundary.

- However, both plans include minor deficiencies that need to be corrected (see table 1):
  - The initial security plan had minor deficiencies that impacted the assessment of two security control enhancements during the certification.
  - The updated security plan provided to the authorizing official has minor deficiencies in security control descriptions. The deficiencies may impact the quality of future continuous monitoring assessments.

Recommendation

1.1 Census should ensure that security plan deficiencies in table 1 are corrected.

Census Response

Census concurred with this finding and our recommendation.

2. Census Has Not Established, Implemented, and Assessed Secure

Background: Our FY 2008 report on FDCA, FY 2008 FISMA Assessment of Field Data Collection Automation System (CEN22), *found that "secure configuration settings were defined and assessed for some IT products, but improvements are needed."*

We recommended that "Census should ensure that secure configuration settings are defined, implemented, and assessed for all IT products in the system accreditation boundary in accordance with NIST SP 800-70, Security Configuration Checklists Program for IT Products*."*

In response to our report, Census provided an action plan that included a POA&M item to implement the recommendation by May 29, 2009. We concurred with the action plan.

- Census did not follow its action plan to fully implement secure configuration settings.
  - FDCA now has secure configuration settings established for fewer IT products than in the previous year.
    - Our FY 2008 evaluation of FDCA found secure configuration settings were established for 10 out of 13 IT products.
    - Currently, only the following 8 of 47 IT products have adequately established secure configuration settings.
      - [redacted]
    - Significant examples of the 39 IT products that did not have established settings are
      - [redacted]
    - The FDCA system changed significantly since the May 30, 2007, authorization to operate. Therefore, the established secure configuration settings were no longer accurate, resulting in fewer established settings. In addition, many more IT products were added to the system, resulting in the change from 13 to 47 total IT products.
    - The security assessment report (SAR) and POA&M fully informed the authorizing official concerning the lack of secure configuration settings.

- Secure configuration settings were assessed for seven of the eight IT products that had adequate secure configuration settings established. However, the secure configuration settings for [redacted] were not assessed because the certification team did not consider the settings documented sufficiently to perform an assessment.
    - However, the secure configuration settings for this product were identified, necessary deviations were documented, and justifications for deviations were included. Therefore, these secure configuration settings were established enough to assess, and they should have been assessed.

Recommendation

2.1 Census should ensure that secure configuration settings are established, implemented, and assessed for all IT products in the system accreditation boundary in accordance with NIST SP 800-70, *Security Configuration Checklists Program for IT Products.*

Census Response

Census concurred with this finding and our recommendation.

3. Security Control Assessments Were Generally Adequate, but

- Security control assessment results were generally supported by adequate evidence.
- Vulnerabilities identified during assessments were reported to the authorizing official via the SAR and the POA&M.
- Assessment procedures were generally tailored to the system specific implementation of security controls.
- Security control assessments included most IT products that implement security controls.
  - However, assessments were not performed on a representative set of some components even though the certification team was aware that these assessments were lacking:
    - [redacted] at Local Census Offices (LCOs); this issue was reported in the SAR.
    - [redacted]
    - [redacted] were not included in all assessments for the following controls because assessment scanning did not include them. However, it is important to note that these assessments were performed for similarly configured non-production [redacted] POA&M item 1284 addresses this issue.
      - [redacted]
- Results for 34 of the 182 security control assessments we evaluated were not adequate (see table 2 for examples).
- No assessments were performed to determine if the [redacted] was implemented on the network switches and firewalls that rely on [redacted].
  - The FDCA switches and firewalls rely on [redacted] servers to implement requirements for the following security controls.
    - [redacted]

    - [redacted]
    - [redacted]
  - However, [redacted] was not implemented on one of the switches or on the web console interface for two firewalls.

- Some security control assessment evidence collected during security certification was not collected by an independent assessor.
  - In late February 2009, Census determined that some security control assessments were incomplete or inadequate.
  - To correct missing and inadequate assessments, Census requested that the FDCA system administration staff produce and deliver evidence such as screenshots, audit logs, and configurations for 21 of 47 system components.
    - The collection of evidence was not observed by an independent assessor, such as a member of the certification team.
  - However, it is unlikely that the integrity of the evidence was compromised during this certification because
    - the evidence clearly depicted numerous system vulnerabilities, and
    - the FDCA configuration management process prohibits even minor changes without approval of one or more change control oversight groups, thus reducing the likelihood that temporary configuration changes were made to produce more favorable evidence.

Recommendations

Census should ensure that

3.1 security control assessments for certification are completed before making certification recommendations; and
3.2 the collection of evidence to support certification assessments is performed by an independent assessor.

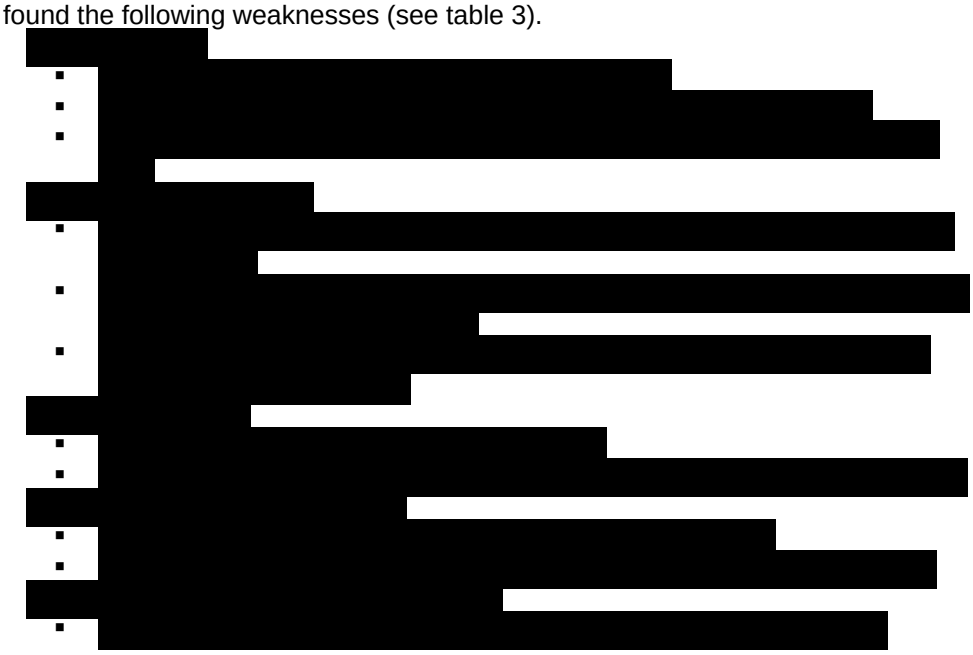
Census Response

Census concurred with this finding and our recommendations.

4. OIG Control Assessment Found Vulnerabilities Requiring

As part of OIG's FY 2009 FISMA evaluation of the FDCA system, we selected and assessed system components and security controls that would allow us to determine the effectiveness of security features that the certification agent noted provide layers of security redundancy.

- We found the following weaknesses (see table 3).
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]



Recommendation

4.1 Census should ensure the vulnerabilities we identified in table 3 are added to the system's POA&M and either remediated or accepted by the authorizing official.

Census Response

Census concurred with this finding and our recommendation.

5. Overstating Compensating Security Features and Downplaying

Background: The certification recommendation of June 17, 2009, acknowledges numerous and significant vulnerabilities. The SAR includes the following:

- *261 high-impact vulnerabilities represented by 16 distinct weaknesses affecting numerous IT products (for example, the occurrence of the same weakness on 35 different IT products resulted in 35 vulnerabilities)*
  - *Impact statements for these weaknesses indicate that*
    - [redacted]
    - [redacted]
    - [redacted]
- *348 moderate-impact vulnerabilities represented by 20 distinct weaknesses affecting numerous IT products*
  - *Impact statements for these weaknesses indicate that*
    - [redacted]
    - [redacted]
    - [redacted]
    - [redacted]

The certification recommendation points out that in spite of these deficiencies, layers of security redundancy and enhanced security features often compensate for other less-secure features (see appendix C, section 1, for the recommendation's text describing these compensating security features).

In communications with the OIG, the FDCA certification agent further explained what specific features compensate for the numerous remaining deficiencies (see appendix C, section 2, for the certification agent's statement).These features can be categorized into two sets. The certification agent stated that the first set, which consists of the following features, reduces the likelihood that compromise to low priority applications can be escalated into an attack against the system:

- [redacted]
- [redacted]
- [redacted]

He further stated that the second set, consisting of the following features, makes it much more difficult to obtain sensitive FDCA data:

- [redacted]
- [redacted]
- [redacted]
- [redacted]

- Our assessment of security controls, coupled with certification findings, shows only three of the seven security features compensating for numerous system vulnerabilities are in place:
  - [redacted]

- o [redacted]
- o [redacted]

- We concluded that four of the security features identified as compensating for numerous system vulnerabilities were overstated and are not fully in place.
  - o [redacted]
  - o [redacted]
  - o [redacted]
  - o [redacted]

- FDCA is mission critical and required to support decennial field operations whose schedule could not be delayed; therefore, it should have been permitted to operate with an interim rather than full authorization because of the minimal progress in correcting numerous and significant vulnerabilities.
  - In the certification recommendation memo, the certification agent explained, "As a result of my review of the completed C&A package and given both the mission-criticality of the system and the progress made by the FDCA team on correcting identified system vulnerabilities, I recommend this system be issued an authorization to operate from the date of this memo through June 17, 2012."
    - Although the mission criticality of a system is relevant to the decision to issue an interim authorization to operate, it should not be used to support a decision to approve full authorization.
    - NIST 800-37 states that an authorization to operate is issued when "the authorizing official deems that the risk to agency operations, agency assets, or individuals is acceptable," whereas interim authorizations to operate are issued when "risk to agency operations, agency assets, or individuals is unacceptable, but there is an overarching mission necessity to place the system into operation, or continue its operation."

  - Progress correcting numerous and significant vulnerabilities was minimal.
    - In a certification status memo issued on April 22, 2009, the certification agent informed the authorizing official that approximately 1,100 findings resulted in formal POA&Ms (approximately 290 high-, 350 moderate-, and 480 low-risk POA&Ms). The certification agent considered this number very high.
    - The June 17, 2009, certification memo explained that only 164 of these POA&Ms (83 high-, 8 moderate-, and 73 low-risk POA&Ms) had been corrected.[1]

- In spite of numerous and significant deficiencies, the authorizing official asserted in the memo granting authorization to operate that the risks to agency operations, agency assets, or individuals resulting from the operation of the information system were low.
  - Certification security control assessment results found that most of the security controls are either not in place or are not operating effectively.
    - Only 638 out of 1,781 instances of security controls implemented on applicable IT products were in place and operating effectively.
  - The certification agent informed the authorizing official that numerous vulnerabilities remained.
    - Although some progress to correct outstanding POA&Ms had been made, it does not justify labeling system operation risk as low.

Recommendations

Census should

5.1 verify the effectiveness of security features before stating they compensate for known weaknesses and thereby reduce overall system risk; and

5.2 report FDCA's accreditation status as an interim authorization to operate and specify appropriate terms and conditions to remediate identified high-risk vulnerabilities, or ensure the security features compensating for known vulnerabilities are working effectively.

Census Response

Census concurred with this finding but only partially concurred with our second recommendation to report FDCA's accreditation status as an interim authorization to operate. In its response, Census explained that it concurs with our recommendation based on our observation, but states that since the Authority to Operate was granted, significant progress has been made in addressing the vulnerabilities noted. In addition, the authorizing official is briefed weekly on the progress of correcting the remaining vulnerabilities. As an alternative to our recommendation, Census explained its planned corrective action: if after 90 days, the authorizing official feels that adequate progress has not been made, the authorization to operate will be rescinded and an interim authorization to operate will be issued.

OIG Comments

After reviewing Census's planned action to address the recommendation, we conclude that the action is reasonable and responsive.

[1] Following the exit conference, Census provided details showing that as of September 25, 2009, 368 out of 1172 POA&Ms (114 high-, 91 moderate-, and 163 low-risk POA&Ms) have been corrected.

Table 1. **Deficiencies in System Security Plans**

Control	NIST SP 800-53 Requirement	Deficiencies	
		Initiation Phase Plan	Certification Phase Plan
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Table 1. **Deficiencies in System Security Plans**

Control	NIST SP 800-53 Requirement	Deficiencies	
		Initiation Phase Plan	Certification Phase Plan
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]		[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Table 1. **Deficiencies in System Security Plans**

Control	NIST SP 800-53 Requirement	Deficiencies	
		Initiation Phase Plan	Certification Phase Plan
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Table 2. **Examples of Inadequate Assessment Procedures.**

Control	NIST 800-53 Requirement	Assessment Results (Full Quotation)	IT Product	OIG Comments
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Table 2. **Examples of Inadequate Assessment Procedures.**

Control	NIST 800-53 Requirement	Assessment Results (Full Quotation)	IT Product	OIG Comments
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Table 2. **Examples of Inadequate Assessment Procedures.**

Control	NIST 800-53 Requirement	Assessment Results (Full Quotation)	IT Product	OIG Comments
		[redacted]		

Table 2. **Examples of Inadequate Assessment Procedures.**

Control	NIST 800-53 Requirement	Assessment Results (Full Quotation)	IT Product	OIG Comments
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Table 2. **Examples of Inadequate Assessment Procedures.**

Control	NIST 800-53 Requirement	Assessment Results (Full Quotation)	IT Product	OIG Comments
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Table 3. **Vulnerabilities Found by OIG Assessment.**

Control	IT Product	Vulnerability
[redacted]	[redacted]	[redacted]

Table 3. **Vulnerabilities Found by OIG Assessment.**

Control	IT Product	Vulnerability
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Appendix A: Census's Response to Findings

UNITED STATES DEPARTMENT OF COMMERCE
The Under Secretary for Economic Affairs
Washington, D.C. 20230

MEMORANDUM FOR: Allen Crawley
Assistant Inspector General for Systems Acquisition
and IT Security

FROM: Rebecca M. Blank
Under Secretary for Economic Affairs

SUBJECT: FY 2009 FISMA Assessment of the Field Data Collection Automation System (CEN22)
Draft Report No. OAE-19728/October 2009

Below are the Office of the Inspector General's recommendations for the five findings identified during the FY 2009 FISMA Assessment of the Field Data Collection Automation System (CEN22), Draft Report No. OAE-19728, and the agency responses.

The Field Data Collection Automation (FDCA) System supports the 2010 Census field operations. The U.S. Census Bureau appreciates the review of this system and continues to take steps to improve the security posture of the system. As stated in last year's response, this assessment followed Census Bureau certification and accreditation (C&A) methodology. Also, the program area is following the Census Bureau continuous monitoring program to address vulnerabilities noted and to reduce residual risk to the system.

Findings and Recommendations

1. System Security Plans Were Generally Adequate, But Some Minor Improvements Are Needed. *1.1 Census should ensure that security plan deficiencies in table 1 are corrected.*

Census Response: Census accepts the finding and recommendation. See Table 1 (attached) for itemized responses. A POA&M was created for updating the System Security Plan and specifically addresses the deficiencies identified. (POA&M ID 39926).

2. Census Has Not Established, Implemented, and Assessed Secure Configuration Settings for All IT Products. *2.1 Census should ensure that secure configuration settings are established, implemented, and assessed for all IT products in the system accreditation boundary in accordance with NIST SP 800-70, Security Configuration Checklists Program for IT Products.*

ECONOMICS AND STATISTICS ADMINISTRATION

Census Response: Census accepts the finding and recommendation. Census will document baselines for all components in accordance with the BOC Secure Configuration Policy v.1.1. Secure baselines have been documented for [redacted] and [redacted] application. There are POA&Ms in progress for [redacted].

3. Security Control Assessments Were Generally Adequate, but Improvements Are Needed. *Census should ensure that (3.1) security control assessments for certification are completed before making certification recommendations; and (3.2) the collection of evidence to support certification assessments is performed by an independent assessor.*

Census Response: Census accepts the finding and recommendation. Census updated System Testing and Evaluation (ST&E) procedures to conform to NIST SP-800-53A. Census is creating custom test procedures for each system by defining test objectives that address each requirement of a security control. Each defined objective must be addressed before test cases can be completed. See Table 2 for specific responses to examples presented.

4. OIG Control Assessment Found Vulnerabilities Requiring Remediation. *4.1 Census should ensure the vulnerabilities we identified in table 3 are added to the system's POA&M and either remediated or accepted by the authorizing official.*

Census Response: Census accepts the finding and recommendation. Of the 8 NIST SP-800-53 control families that had weaknesses reported, two were corrected and one was partially corrected during the audit fieldwork. The OIG was provided with evidence to support weaknesses identified related to [redacted]

Weaknesses in four of the control families were mapped to existing POA&Ms for [redacted] The language of those specific POA&Ms has been updated in CSAM to ensure that the weaknesses identified in Table 3 of the report are explicitly addressed.

[redacted]

5. Overstating Compensating Security Features and Downplaying Numerous Vulnerabilities Led to an Ill-Advised and Inappropriate Authorization Decision. *Census should (5.1) verify the effectiveness of security features before stating they compensate for known weaknesses and thereby reduce overall system risk; and (5.2) report FDCA's accreditation status as an interim authorization to operate and specify appropriate terms and conditions to remediate*

identified high-risk vulnerabilities, or ensure the security features compensating for known vulnerabilities are working effectively.

Census Response:

Census accepts the finding. However, in reviewing the recommendation, the Authorizing Official (AO) has decided not to accept the recommendation for the following reasons. The C&A process provides a snapshot in time of the security posture of an IT system. While Census concurs with the OIG's recommendation based on the OIG's observations, the Census Bureau feels that since the Authority to Operate (ATO) was granted, the program area and contractor have made significant progress addressing the vulnerabilities noted. While a great number of POA&Ms still remain, the AO now receives weekly briefings on the progress of closing the remaining vulnerabilities and will review the status in 90 days to ensure that adequate progress has been made in decreasing the residual risk. If at the time the AO feels adequate progress has not been made, the ATO will be rescinded and an Interim ATO will be issued.

ITSO:JMMcKenzie:10/28/09
CQAS:Review:kem:10/28/09
CQAS #53621
CQAS: Final: lah: 11/4/09

cc: US/EA, Mr. Ruland, Mr. McGrath, A. Moxam, T. Johnson, N. Gordon, H. Hogan, M. Matos

Attachment

Table 1. Deficiencies in System Security Plans – Census Response

Control #	IT Product (if applicable)	Finding	Response
[redacted]			

Control #	IT Product (if applicable)	Finding	Response
[redacted]			

Table 2. Examples of deficiencies in Security Assessment Controls – Census Response

Control #	IT Product (if applicable)	Finding	Response
[redacted]			

3

Appendix B: Objectives, Scope, and Methodology

To meet the FY 2009 Federal Information Security Management Act (FISMA) reporting requirements, we evaluated the Census Bureau's certification and accreditation (C&A) for the Field Data Collection Automation (FDCA) system (CEN22).

Security C&A packages contain three elements, which form the basis of an authorizing official's decision to accredit a system:

- The **system security plan** describes the system, the requirements for security controls, and the details of how the requirements are being met. The security plan provides a basis for assessing security controls and also includes other documents such as the system risk assessment and contingency plan, per Department policy.
- The **security assessment report** presents the results of the security assessment and recommendations for correcting control deficiencies or mitigating identified vulnerabilities. This report is prepared by the certification agent.
- The **plan of action and milestones** is based on the results of the security assessment. It documents actions taken or planned to address remaining vulnerabilities in the system.

The Department's *IT Security Program Policy and Minimum Implementation Standards* requires that C&A packages contain a certification documentation package of supporting evidence of the adequacy of the security assessment. Two important components of this documentation are

- the **certification test plan**, which documents the scope and procedures for testing (assessing) the system's ability to meet control requirements; and
- the **certification test results**, which are the raw data collected during the assessment.

To evaluate the C&A, we reviewed all components of the C&A package and interviewed Census staff and contractors to clarify any apparent omissions or discrepancies in the documentation and to gain further insight on the extent of the security assessment. We evaluated the security plan and assessment results for applicable security controls and will give substantial weight to the evidence that supports the rigor of the security assessment when reporting our findings to OMB.

In addition, we performed our own assessment of a targeted selection of controls (see appendix B-1). We conducted our assessment using a subset of procedures from National Institute of Standards and Technology Special Publication (NIST SP) 800-53A, which we tailored to FDCA's specific control implementations. We did not attempt to perform a complete assessment of each control; instead, we chose to focus on specific technical and operational elements.

We assessed controls on key classes of IT components, choosing a targeted set of components from each class that would allow us to determine the effectiveness of security features that the certification agent noted provide layers of security redundancy. We assessed configuration settings on operating systems including [redacted]

We also assessed configurations on IT products including [redacted] We also included an examination of [redacted]

Our assessment included the following activities:

- extraction, examination, and verification of system configurations
- execution of scripts and manual checklists
- examination of system logs
- review of account management procedures
- examination/analysis of security plan descriptions, including related policy and procedure documents
- interviews of appropriate Census personnel and contractors

Our assessment was limited in scope and should not be interpreted as the comprehensive review that a security certification for a [redacted] system would require. It gave us direct assurance of the status of select aspects of important system controls and provided meaningful comparison to Census's security certification.

We used the following review criteria:

- Federal Information Security Management Act of 2002
- U.S. Department of Commerce *IT Security Program Policy and Minimum Implementation Standards*, June 30, 2005
- NIST Federal Information Processing Standards
  - Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*
  - Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*
- NIST Special Publications:
  - 800-18, *Guide for Developing Security Plans for Information Technology Systems*
  - 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*
  - 800-53, *Recommended Security Controls for Federal Information Systems*
  - 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*
  - 800-70, *Security Configuration Checklists Program for IT Products*
  - 800-115, *Technical Guide to Information Security Testing and Assessment*

We conducted our evaluation in accordance with the Inspector General Act of 1978, as amended, and the *Quality Standards for Inspections* (revised January 2005), issued by the President's Council on Integrity and Efficiency.

Appendix B-1: NIST SP 800-53 Security Controls Assessed by OIG

- AC-2 Account Management
- AC-6 Least Privilege
- AC-7 Unsuccessful Login Attempts
- AC-11 Session Lock
- AC-17 Remote Access
- AU-2 Auditable Events
- AU-4 Audit Storage Capacity
- AU-6 Audit Monitoring, Analysis, and Reporting
- AU-8 Time Stamps
- AU-9 Protection of Audit Information
- CM-6 Configuration Settings
- CM-7 Least Functionality
- IA-2 User Identification and Authentication
- IA-5 Authenticator Management
- SC-7 Boundary Protection
- SI-2 Flaw Remediation
- SI-3 Malicious Code Protection

Appendix C: Certification Agent Statements Concerning Compensating

Section 1: Statement describing compensating security features, taken as an excerpt from the June 17, 2009, certification recommendation sent to the authorizing official:

> In spite of the remaining deficiencies, the generally well-designed and centrally managed FDCA architecture has layers of security redundancy that partially mitigate the potential damage possible during a security breach. In many cases, security mechanisms much stronger than those required by FISMA were leveraged to accomplish functions [redacted] These enhanced security features, such as [redacted] often compensated for other less secure features deployed elsewhere in the environment.

Section 2: Statement describing compensating security features, taken as an excerpt from July 23, 2009, e-mail communication with the OIG:

> The "enhanced security features" mentioned in paragraph 12 of the certification memo act as compensatory mechanisms for some of the weaker elements deployed in the FDCA environment by limiting the potential damage from an exploitation of system vulnerabilities rather than by providing directly equivalent security controls for the weak components. When viewed from an overall system risk perspective, [redacted] implemented on the core infrastructure components of the FDCA system serve to reduce the likelihood that an attempt to compromise a low priority application [redacted] could be escalated into an attack against the system as a whole.
>
> While the individual component may suffer a compromise of low-impact data, the more sensitive information related to the Census mission is much more difficult to obtain. Access to that type of information is controlled, in most part, by the server, database, [redacted] and telecom environments. Although these environments may not have formally completed the [redacted] required by the bureau, they have implemented a [redacted] that not only implements additional security controls not required by FISMA, but it is also effectively managed by a thorough and timely [redacted] process. For instance, the use of [redacted] and communication control on the telecom devices reduces the likelihood that an attacker could stage a [redacted]. The [redacted] which are not required by policy, help to ensure that only [redacted]. Likewise, the use of [redacted] partially mitigates the device's portability and exposure to potential loss; the strength of the [redacted] nearly eliminates an attacker's ability to penetrate the device, even with direct and unlimited access to the [redacted]