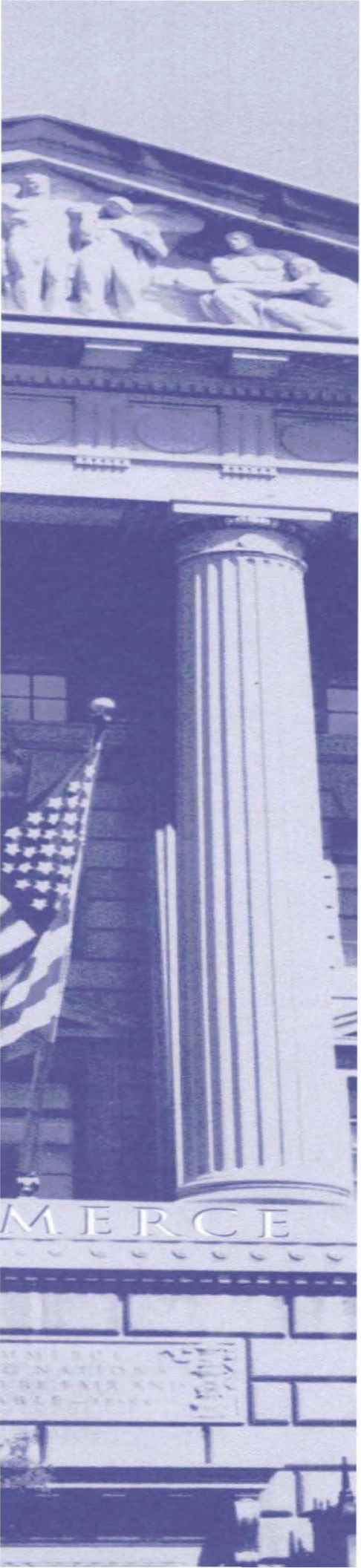

U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

U.S. Census Bureau

Respondent Data Safeguards in the Decennial Response Integration System (DRIS)

Final Report No. OAE-19888
September 2010

Office of Audits and Evaluation

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

September 24, 2010

MEMORANDUM FOR: Rebecca M. Blank
Under Secretary for Economic Affairs
U.S. Department of Commerce

Dr. Robert Groves
Director
U.S. Census Bureau

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

SUBJECT: Respondent Data Safeguards in the Decennial Response Integration System (DRIS)
Final Report OAE-19888

Attached please find the final report of our assessment of respondent data safeguards in the Decennial Response Integration System (DRIS). This was the first 2010 Decennial Census system for which we evaluated information technology (IT) security controls. Our review of other systems is ongoing and the results from that work will be included in our FY 2010 FISMA audit report and report to OMB. We identified vulnerabilities in DRIS security controls that required corrections in order to ensure the system adequately safeguarded respondent data. However, we acknowledge that, even before the corrections, DRIS had security features that significantly mitigated risk. In addition, we identified a weakness in the system's definitions for secure configurations that suggests the need for increased management attention to future contractor systems.

Census, in its response, indicated that all but one of the vulnerabilities we identified had been remediated (its contractor began corrections after we briefed Census and the contractor on our preliminary findings), and that DRIS completed data capture and telephone operations with no reported security breaches. According to the bureau, it also intends to develop a strategy to ensure that requirements for secure configurations are more clearly mandated for future contractor systems. In this regard, please submit to us an action plan, or the documented strategy, within 60 days of the date of this memorandum.

We appreciate the cooperation and courtesies extended to us by your staff during our evaluation. If you have any questions or concerns about this report, please do not hesitate to contact me at (202) 482-1855.

cc: Simon Szykman, Chief Information Officer, Department of Commerce
Thomas L. Mesenbourg, Jr., Deputy Director and Chief Operating Officer, U.S. Census Bureau
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
Tracy Wessler, DRIS Program Manager, U.S. Census Bureau
Timothy P. Ruland, Chief, Information Technology Security Office, U.S. Census Bureau
Jean McKenzie, Census audit liaison

Report In Brief

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

September 2010

Why We Did This Review

As part of our oversight of the 2010 Decennial Census, we evaluated whether required controls meant to serve as safeguards over electronic respondent data in the Decennial Response Integration System (DRIS) were effectively meeting data security requirements.

Background

DRIS is a contractor-operated system, currently in the process of being decommissioned, that supported the 2010 Decennial Census by converting paper-based responses into electronic form and transmitting the data, encrypted, to Census for further processing. It also provided telephone questionnaire assistance through interactive voice response and call center staff to help callers complete Census forms. Further, it followed up on coverage of respondents who submitted incomplete information; operators then updated the response database. A separate contractor sampled response data to independently verify the accuracy of the conversion from scanned paper forms to electronic data. These operations have been completed.

DRIS was effectively separated from the Internet; users had limited access to respondent data. However, the system had been certified and accredited almost 2 years before it began operating, raising the potential for unidentified vulnerabilities without rigorous, continuous monitoring.

U.S. Census Bureau

Respondent Data Safeguards in the Decennial Response Integration System (DRIS) (OAE-19888)

What We Found

Overall we found vulnerabilities in DRIS security controls that should normally have been remediated; however, several factors existed that significantly mitigated the risk of a security breach: the system was not accessible from the Internet, and user interfaces limited access to respondent data. We also identified a weakness in the system's definitions for secure configurations that suggests the need for increased management attention to future contractor systems. The table below describes these findings at a glance:

Finding	Examples
Vulnerabilities existed in system components.	• Malicious code could be introduced through removable media (e.g., USB thumb drives) • Default password • Database users were granted excessive access • Lack of logging of security-related events • Some network components were running prohibited services
Configuration settings were not adequately defined and documented. (Department policy requires this for hardening systems against cyber attacks.)	Checklists of secure settings for various technologies were incomplete or lacked an appropriate benchmark; for one class of servers, a checklist was not defined.

What We Recommend

We recommend that, for future contractor systems, the Census Bureau ensure that configuration settings for IT products be defined, documented, and implemented in accordance with Department policy. We make no recommendation with respect to system vulnerabilities because the system has concluded operations and is in the process of being decommissioned. Further, Census indicated, in response to our draft report, that its contractor had remediated all but one of the vulnerabilities (the remediation began shortly after our initial fieldwork in March 2010.)

INTRODUCTION

As part of our oversight of the 2010 Decennial Census and our obligations under the Federal Information Security Management Act of 2002 (FISMA), we evaluated the Decennial Response Integration System's (DRIS) safeguards for electronic respondent data. Our objective was to determine whether required controls were effectively meeting security requirements so that confidential respondent data were adequately protected. Our detailed scope and methodology are included as Appendix I. DRIS operations have now concluded and the system is in the process of being decommissioned.

DRIS is a contractor-operated[1] system that converted paper-based census questionnaire responses into electronic form and transmitted the data to the Census Bureau for further processing. DRIS also provided telephone questionnaire assistance in which an interactive voice response application and call center staff provided assistance to callers in completing census forms. The "telephony channel" also included a "coverage follow-up" operation in which call center operators interviewed respondents who provided incomplete information on census forms; the operators then updated the response database. In addition, DRIS had a "paper data quality" function, in which a separate contractor independently sampled response data to determine the accuracy of the conversion from scanned paper forms to electronic data.

DRIS transmitted encrypted respondent data to the Census Bureau. Key security features included its architecture and application design, which effectively separated the system from the Internet and limited access to respondent data to authorized users who typically received the data one "case" at a time, through a controlled user interface.

Census certified and then accredited DRIS in March 2008, nearly 2 years prior to system operations, which began in February 2010. This FISMA-required process identifies vulnerabilities and leads to management's acknowledgement and acceptance of the risk of operating the system. The early accreditation, before the system was fully deployed, raised the potential for unidentified vulnerabilities without a rigorous continuous monitoring program.

Under 13 U.S.C. § 9, Census must use confidential information for the statistical purposes for which it is supplied, must not make any publication that would identify the data furnished by a particular respondent, and must not permit unauthorized persons to examine individual reports. In furtherance of these limitations, authorized persons must have a work-related need to know to use the data. The oath taken by authorized persons to uphold the confidentiality of census information is a lifetime obligation. Census has an unauthorized-browsing policy that prohibits searching or looking through, for other than work-related purposes, protected information that directly or indirectly identifies individual persons or businesses. The removal of confidential data from the bureau in the form of memory sticks, CDs, or other electronic media is also prohibited.

[1] The DRIS contractor, Lockheed Martin, previously supported the paper data capture component during the 2000 Decennial Census.

SUMMARY

DRIS had security features in place that significantly mitigated risk, yet vulnerabilities remained that required correction to ensure that DRIS adequately safeguarded respondent data. There were a number of factors—in particular, that the system was not accessible from the Internet and user interfaces limited access to respondent data—that significantly mitigated the risk of a security breach. We identified a weakness in the system's definitions for secure configurations that suggests the need for increased management attention to future contractor systems. We communicated to Census officials the security issues identified throughout our review; in many instances, Census and the DRIS contractor said that they addressed these security issues. We did not, however, independently validate their assertions.

The table below summarizes our findings with recommendations:

Finding	**Examples**	**Recommendation**
Vulnerabilities existed in system components.	• Malicious code can be introduced through removable media (e.g., USB thumb drives) • Default password not changed • Database users granted excessive access • Security-relevant events not logged • Some network components running prohibited services	(None.) In response to our draft report, Census asserted that, with the exception of excessive access granted to database users, these vulnerabilities have been remediated; the system is in the process of being incrementally decommissioned.
Configuration settings were not adequately defined and documented. (Department policy requires this for hardening systems against cyber attacks.)	• Checklists of secure settings for various technologies were incomplete or lacked an appropriate benchmark; for one class of servers, a checklist was not defined.	For future contractor systems, configuration settings for IT products should be defined, documented, and implemented in accordance with Department policy.

FINDINGS AND RECOMMENDATIONS

Vulnerabilities in Key Technologies Needed to Be Addressed to Ensure That Respondent Data Were Adequately Protected

While we identified vulnerabilities in DRIS controls, a number of factors, including its separation from the Internet and users' limited interface, compensated for those weaknesses and reduced the likelihood of a data breach. We have since shared with Census all control assessment findings, and Census and the DRIS contractor have indicated that most of the issues have been corrected. In some instances, however, according to the contractor, the workload at the peak of production was too great to risk implementing corrections that could have impacted system performance. Based on our understanding of the system and operations, these particular remaining vulnerabilities did not pose undue risk.

Vulnerabilities Existed in System Components

Vulnerabilities were evident in DRIS protections against malicious code that can be introduced through removable media such as USB thumb drives. Windows®-based servers and workstations in the system's telephony channel and the paper data quality segment were not configured to prevent removable media devices from automatically executing code stored on the devices. In addition, none of the system's Windows-based components had a Microsoft®-issued patch that is required to effectively disable the ability of removable media to automatically execute code. We successfully exploited this flaw in the DRIS laboratory environment, which was also not patched, demonstrating the potential for malicious code to be introduced via removable media.

Another vulnerability existed with database management systems, including one that managed the respondent database: a default password for a highly privileged account was not changed. After we promptly notified Census of this finding, the bureau informed us that the default password was stored in an unused repository and that database administrators logged in using a separate mechanism and different password. Census therefore believed the finding was a "false positive." However, Department policy requires default account passwords to be changed; we found that other default account passwords in the same repository had been changed previously. Changing default passwords is a fundamental security practice, and the existence of a default password does present the potential for misuse. Census told us that the DRIS contractor has since changed the default password in question.

Database users were granted excessive privileges according to both an industry benchmark and DRIS's own checklist. According to Census officials and the DRIS contractor, they planned to evaluate the necessity of modifying these settings in the DRIS databases. In response to other database issues that we identified, the DRIS contractor did not intend to make modifications because doing so may have affected the systems' ability to process millions of transactions daily. Based on our understanding of the system and operations, we believe leaving these vulnerabilities uncorrected did not pose undue risk.

Domain controllers that we sampled, which implemented security policy for much of DRIS, were not auditing events that are identified in the system security plan as significant and relevant to system security. According to the DRIS contractor, this was the result of conflicting policies being applied to the domain controllers; the contractor said, however, that it would work to resolve the issue. Likewise, scans revealed that workstations' audit settings were not in compliance with the Federal Desktop Core Configuration (FDCC).[2] A significant number of noncompliant settings were discovered in components of the paper data quality function (three workstations from our sample of eight components accounted for 56 percent of the discrepancies).

Two other vulnerable settings in servers running Windows operating systems had the potential to allow an attacker immediate access into a machine or allow highly-privileged access. The DRIS contractor initially said that the settings were necessary for compatibility with legacy applications, but later said that the software had since been updated and should no longer be incompatible. More recently, the contractor told us that it had successfully tested more secure settings in its lab environment and planned to implement the settings in production.

Routers and switches were running insecure services as defined by an industry benchmark and DRIS's own network design document. We shared our detailed findings with Census and the DRIS contractor. In response, the contractor planned to modify the settings to comply with the industry benchmark and update the DRIS network design document.

In general, firewall configurations were consistent with baseline rules captured in DRIS's configuration management system. We shared our detailed findings with Census and the DRIS contractor; where there were discrepancies, the contractor planned to correct the running configurations or update the baseline as necessary. Of the discrepancies, the most common was one that would omit logging of unauthorized traffic attempting to pass through a firewall—something that would have assisted in detecting malicious activity.

Configuration Settings Were Not Adequately Defined and Documented

Configuration settings of DRIS's IT products, required to be at the most restrictive mode consistent with operational requirements, were not defined and documented according to Department policy. DRIS's checklist for databases addressed only 3 of the 13 sections (74 of the 277 potential settings—27 percent) of the industry benchmark that the DRIS contractor said was the basis for the checklist. Windows operating system settings were better defined than other IT products in the system, but ambiguities existed. According to Census, Windows components, including servers, were configured according to the FDCC. However, documented deviations from it were not completed; many settings were marked "not configured–need more testing." And FDCC is intended for workstations, not servers. For routers and switches, a network design document addressed a very small subset of benchmark settings (insecure services); in practice,

[2] Office of Management and Budget, Executive Office of the President, OMB Memorandum No. 08-22, *Guidance on the Federal Desktop Core Configuration (FDCC)* (2008). The FDCC is an OMB-mandated security configuration for Windows XP and Windows Vista operating systems.

the design document was not followed. Likewise, the DRIS contractor's security configurations document for servers running a UNIX®-based operating system did not constitute properly-defined settings.

In general, Commerce policy requires that a secure benchmark (typically from industry) be used as a starting point and that deviations from the benchmark then be documented to produce the system's tailored checklist of configuration settings for a given IT product. This provides assurance that the system has been appropriately hardened and promotes unambiguous assessment of component security.

Illustrating the issue, we found a file transfer protocol (FTP[3]) server, which could have presented a security risk, running on a UNIX-based server, yet the DRIS contractor told us that it should not have been. However, the contractor's security configurations document for its UNIX-based systems did not prohibit or otherwise address FTP servers. If it had, this server would have been in clear violation of the allowed settings and services, which Department policy requires be defined. Implementing and maintaining secure configuration settings is one of the most effective ways of negating threats. Adequately defining configuration settings has been an issue we have raised in previous Census reviews.

Recommendation

We recommend that Census ensure that, for future contractor systems, configuration settings for IT products be defined, documented, and implemented in accordance with Department policy.

[3] FTP is a communications protocol governing the transfer of files from one computer to another over a network.

Summary of Census Comments and OIG Response

In response to our draft report, Census did not dispute our findings and indicated agreement with our recommendations, only one of which remains for the final report. The draft report recommended that vulnerabilities that we identified be promptly remediated; the bureau asserted that all but one of the vulnerabilities had been. Census's response suggests that the remaining vulnerability—excessive privileges granted to database users—is no longer a concern because the system is now in the process of being incrementally decommissioned and database users no longer exist. The bureau further stated that the "DRIS program conducted the 2010 Decennial Census paper data capture and telephone operations with no reported security breaches."

With respect to configuration settings, the bureau explained that these requirements were not clearly mandated through contractual terms and that it will develop a strategy to ensure that future contractor systems will be required to comply. Census also suggested an editorial change, which we have incorporated into this final report. The full Census response is included as Appendix II to this report.

OIG Response

We are pleased that Census and its contractor took steps to remediate the vulnerabilities we identified and agree with the bureau's position regarding the one remaining vulnerability. We look forward to reviewing Census's strategy to ensure that future contractor systems adhere to requirements for secure configuration settings.

APPENDIX I: SCOPE AND METHODOLOGY

Decennial respondent data are the information supplied by individuals on Decennial Census forms, whether mailed in or collected by Census employees. We chose to evaluate safeguards for electronic respondent data because two of our top management challenges facing the Department are the Decennial Census and IT security.

This report presents the results of our evaluation of the Decennial Response Integration System (DRIS), which was the first system in Census' decennial workflow to process, store, and transmit electronic decennial respondent data. DRIS included three paper data capture centers, in Baltimore,[4] Phoenix, and Jeffersonville, Indiana; a teletech center in Denver and call centers at various locations; and an operational command center/program management office in Greenbelt, Maryland.

We determined that this system included confidential respondent data based on interviews and documentation obtained from Census. We then reviewed system documentation and interviewed Census and DRIS contractor employees to determine how respondent data were stored, processed, distributed, and protected. This information was then used in our third, most crucial objective: determining whether required security controls were effectively meeting the security requirements for the data.

We assessed a subset of FISMA- and Commerce-required controls from National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems*: Access Control Policy and Procedures (AC-1), Access Enforcement (AC-3), Information Flow Enforcement (AC-4), Remote Access (AC-17), Auditable Events (AU-2), Configuration Settings (CM-6), Media Access (MP-2), and Transmission Confidentiality (SC-9). We selected these controls for their relation to Title 13 confidentiality requirements and other important aspects of information security. We have been required to report on the status of configuration settings in our annual FISMA report to the Office of Management and Budget.

We visited the DRIS operational command center in Greenbelt, Maryland, to collect security-related data, interview system personnel, and observe system security capabilities. Our assessment included extracting, examining, and verifying system configurations; executing scripts and manual checklists; vulnerability scanning; examining system logs; analyzing the system security plan and related policies and procedures; and interviewing both Census and DRIS contractor personnel.

We used the following criteria:

- Federal Information Security Management Act of 2002 (FISMA), Pub. L. No. 107–347, Title III, §§ 301-302, 44 U.S.C. §§ 3541-3549, 40 U.S.C. § 11331

[4] Actually Essex, Maryland, a Baltimore suburb.

- U.S. Department of Commerce, *IT Security Program Policy*, March 2009 and component Commerce Interim Technical Requirements (CITRs):
  - CITR-001: *Federal Desktop Core Configuration (FDCC)*
  - CITR-005: *Removable Media Devices*

- NIST Federal Information Processing Standards (FIPS):
  - 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:
  - 800-53, Revision 2, *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 II: COMMENTS FROM THE U.S. CENSUS BUREAU

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

SEP 07 2010

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

FROM: Rebecca M. Blank
Under Secretary for Economic Affairs

SUBJECT: Respondent Data Safeguards in the Decennial Response Integration System (DRIS) *Draft Report No. OAE-19888/August 2010*

Below are the Office of the Inspector General's recommendations for the findings identified during the evaluation of the Respondent Data Safeguards in the Decennial Response Integration System (DRIS), Draft Report No. OAE-19888, and the agency responses.

The DRIS system underwent an iterative design and development process. Although the systems were consciously designed within the NIST risk-based framework, this iterative approach sometimes affected the quality of the documentation. Census appreciates the feedback received in this report, and is pleased that the DRIS program conducted the 2010 Decennial Census paper data capture and telephone operations with no reported security breaches.

Comments

Re: Introduction, 5th paragraph. We recommend revising the first three sentences as set forth below. The revisions (a) place all three of the confidentiality limitations in the first sentence, (b) distinguish the work-related need to know policy requirement from the statutorily-based confidentiality limitations by placing this requirement the second sentence, and (c) restate the lifetime requirement in the third sentence.

> "Under 13 U.S.C. § 9, Census must use confidential information for the statistical purposes for which it is supplied, must not make any publication that would identify the data furnished by a particular respondent, and must not permit unauthorized persons to examine individual reports. In furtherance of these limitations, authorized persons must have a work-related need to know to use the data. The oath taken by authorized persons to uphold the confidentiality of census information is a lifetime obligation."

Findings and Recommendations

1. Vulnerabilities existed in system components.

ECONOMICS AND STATISTICS ADMINISTRATION

Census Response: With the exception of the vulnerability of excessive privileges granted to the database users, all other identified vulnerabilities have been remediated at this time. DRIS processing for the 2010 Decennial Census has now been completed, and the system is in the process of being incrementally decommissioned. At this time, the said database users no longer exist.

2. Configuration settings were not adequately defined and documented.

Census Response: While the Census Bureau has IT security standards, policies, and methodologies in place, the application of such standards, policies, and methodologies was not clearly mandated through the contractual terms. Future proprietary systems developed for the Census Bureau will be required to adhere to these standards, policies, and methodologies. Census will develop a strategy to ensure they are implemented, specifically with respect to the secure configuration policy.