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.)