Report in Brief

October 30, 2018

Background

In order to manage the cybersecurity risks of its information technology (IT) systems, the Census Bureau (the Bureau) is required to implement the risk management framework developed by the National Institute of Standards and Technology. The Bureau developed a software application, the Risk Management Program System (RMPS), to automate its implementation of the risk management framework. The Bureau relies upon RMPS to generate reports related to the security status of information systems, including reports that quantify cybersecurity risks. These reports serve as a dashboard for the Bureau's senior managers to make risk-based decisions regarding the operation of their systems. The Bureau's security operations rely upon the use of RMPS for every step of the risk management framework. RMPS has become a critical tool of senior management and IT security staff managing cybersecurity risks. As a result, the effectiveness of the Bureau's risk management program depends heavily on the accuracy and integrity of the information maintained within RMPS.

Why We Did This Review

The objective of this audit was to determine whether the risk management framework methodology adopted by the Bureau presents an accurate picture of cybersecurity risks, including risks associated with common controls, to Bureau management.

CENSUS BUREAU

The Census Bureau Must Improve Its Implementation of the Risk Management Framework

OIG-19-002-A

WHAT WE FOUND

We found that the Bureau did not follow its risk management framework process. Specifically, we found that

1. **The Bureau had not continuously monitored critical security controls and failed to document the resulting risks.** In March 2017, we assessed the Bureau's continuous monitoring of five selected systems and found that the Bureau had not conducted the required periodic reassessments of security controls on these systems for a prolonged period.
2. **Authorizing officials lacked information about significant cybersecurity risks.** Security control implementations had not been described or assessed. Security control assessments were insufficient to ensure the validity, credibility, and utility of the results. RMPS risk scores were not reflective of actual risks, but the Bureau has since made progress with standardized reports.
3. **The Bureau did not effectively manage common controls.** In March 2017, we analyzed a subset of common controls and found that subsystems' inheritance of controls was incorrectly recorded and that Bureau assessments of common controls were ineffective.

WHAT WE RECOMMEND

We recommend that The Bureau's Chief Information Officer do the following:

1. Update the Bureau's Risk Management Framework Methodology to include additional procedures that leverage automated reporting, to ensure that deviations from continuous monitoring plans are reported more timely to senior management designated as the authorizing official and to IT security management.
2. Ensure that management is informed when risks are omitted from RMPS reports.
3. Develop both manual and automated procedures to help ensure that complete descriptions of system security controls are entered into RMPS, reviewed, and approved as part of the system authorization process.
4. Ensure that assessment procedures include provisions (both manual and automated) for quality control associated with the validation of security control assessments.
5. Develop a strategy for periodically verifying the accuracy of common control inheritance within RMPS.
6. Ensure greater rigor in assessment of common control requirements, to include assessing the relationship between the security service provided by the common control requirement and the information system receiving the service.
7. Clearly document the rationale for common control decisions within RMPS.