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

FINAL REPORT NO. OIG-19-002-A

October 30, 2018

U.S. Department of Commerce
Office of Inspector General
Office of Audit and Evaluation

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

October 30, 2018

MEMORANDUM FOR: Ron S. Jarmin
Performing the Non-Exclusive Functions and Duties
of the Director
U.S. Census Bureau

FROM: Frederick J. Meny, Jr.
Assistant Inspector General for Audit and Evaluation

SUBJECT: *The Census Bureau Must Improve Its Implementation of the Risk Management Framework*
Final Report OIG-19-002-A

Attached is our final audit report conducted to determine whether the risk management framework methodology adopted by the Census Bureau (the Bureau) presents an accurate picture of cybersecurity risks, including risks associated with common controls, to Bureau management. Our review primarily focused on the Bureau's use of the Risk Management Program System application to make risk-based decisions.

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, (2) authorizing officials lacked information about significant cybersecurity risks, and (3) the Bureau did not effectively manage common controls.

On September 20, 2018, the Bureau concurred with all of our recommendations. We are encouraged that steps have already been initiated by the Bureau to address our recommendations.

Pursuant to Department Administrative Order 213-5, please submit to us an action plan that addresses the recommendations in this report within 60 calendar days. The final report will be posted on OIG's website pursuant to sections 4 and 8M of the Inspector General Act of 1978, as amended (5 U.S.C. App., §§ 4 & 8M).

We appreciate the cooperation and courtesies extended to us by your staff and bureau staff during our review. If you have any questions or concerns about this report, please contact me at (202) 482-1931 or Clark Morsbach, Director for Audit and Evaluation, at (202) 482-5509.

Attachment

cc: Rod Turk, Acting Chief Information Officer
Kevin Smith, Associate Director for Information Technology and Chief Information Officer
Jeffery W. Jackson, Deputy Chief Information Security Officer
Colleen Holzbach, Program Manager for Oversight Engagement
Jean M. McKenzie, Audit Liaison
Maria Dumas, Audit Liaison, Office of the Chief Information Officer

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.

Contents

Cover: Herbert C. Hoover Building main entrance at 14th Street Northwest in Washington, DC. Completed in 1932, the building is named after the former Secretary of Commerce and 31st President of the United States.

Introduction

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 (NIST).[1] Managing the security posture of the systems under this framework requires an understanding of what security controls are needed and whether they are implemented.

After security controls are selected and implemented, a plan to conduct periodic re-assessments of security controls—referred to as a continuous monitoring strategy—is developed to determine whether the set of deployed security controls continue to be effective over time. The implementation of robust continuous monitoring processes provides senior leaders with the necessary information to make cost-effective, risk-based decisions with regard to the organizational information systems supporting their core missions and business functions.

The Bureau developed a software application, the Risk Management Program System (RMPS), to automate its implementation of the risk management framework. This application supports the collection of information about IT security controls protecting Bureau systems and ranks cybersecurity risks. 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. When the Office of Inspector General (OIG) held the entrance conference for this audit in early 2017, the Bureau was using RMPS to manage security risks for 29 of its systems, comprised of 485 subsystems. RMPS allows the Bureau to manage its large interdependent security portfolio, in which one system or subsystem may build or rely on the security controls provided by others.

To protect Bureau systems, IT security staff use RMPS to identify the required security controls, including common controls (i.e., security controls capable of being inherited by multiple information systems). Systems that rely on common controls also inherit the cybersecurity risks associated with them. The Bureau intended RMPS to allow managers to understand the risks associated with operating these systems, as well as the risks they are inheriting by using security capabilities provided by other systems.

The Bureau's security operations rely upon the use of RMPS for every step of the risk management framework. This includes defining, implementing, assessing, and periodically reassessing security controls. 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.

[1] *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach*, Special Publication 800-37, Rev. 1. June 5, 2014. Gaithersburg, MD: NIST.

Objective, Findings, and Recommendations

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. Our review primarily focused on the Bureau's use of the RMPS application to make risk-based decisions. We briefed the Bureau's IT security management on our initial findings in June 2017 and assessed the corrective actions taken by the Bureau in February 2018. See appendix A for further details regarding our objective, scope, and methodology.

OIG found that the Bureau did not follow its risk management framework process. Specifically, OIG found that (1) the Bureau had not continuously monitored critical security controls and failed to document the resulting risks, (2) authorizing officials lacked information about significant cybersecurity risks, and (3) the Bureau did not effectively manage common controls.

I. The Bureau Had Not Continuously Monitored Critical Security Controls and Failed to Document the Resulting Risks

Ongoing, periodic security control assessments provide a basis for informing management about the current state of security controls protecting IT systems. Agencies are required to conduct an initial assessment of all security controls and then periodically reassess them. A continuous monitoring strategy determines the frequency of periodic reassessments based on the risks or impacts that security controls could have on a system's operation. Here, the Bureau's continuous monitoring policy[2] states that the interval between control assessments cannot exceed 2 years.

In March 2017, OIG assessed the Bureau's continuous monitoring of five selected systems[3] and found that the Bureau had not conducted the required periodic reassessments of security controls on these systems for a prolonged period. A large portion of security control requirements had either never been assessed or had not been assessed within the last 2 years (see table 1).

[2] U.S. Census Bureau Risk Management Program Risk Management Framework Methodology, September 26, 2016.

[3] See appendix A, table A-1, for a description of each system.

Table 1. Controls Not Assessed in Accordance with Bureau Continuous Monitoring Policy for Sampled Systems

	System				
	CEN01	CEN02	CEN03	CEN011	CEN016
Portion of total system controls that had either not been assessed or had not been assessed in the last 2 years	57%	54%	30%	41%	37%

Source: OIG analysis of RMPS data as of March 2017.

In addition, as part of authorizing these systems to operate, Bureau authorizing officials signed documents stating that the Bureau had developed continuous monitoring plans for the systems and that adherence to the plans (i.e., periodic assessments of controls) was a condition for the systems' operation. However, OIG found that the Bureau had not developed continuous monitoring plans for these systems and was not conducting periodic assessments of controls. The Bureau's Chief Information Officer (CIO) and Chief Information Security Officer (CISO) stated that they were unaware that the periodic assessments were not occurring.

In response to OIG's preliminary findings, the Bureau indicated that these deficiencies stemmed from decisions made by its Office of Information Security "that were not appropriately documented or socialized among senior managers" and asserted that continuous monitoring had been "paused" in February 2016. However, OIG found that continuous monitoring has been deficient at the Bureau for potentially much longer than management believed, based on a broader review of continuous monitoring activities across all 29 systems within RMPS as of March 2017. For this review, OIG selected the 20 control requirements[4] that the Bureau had designated as having the highest risk scores—and, therefore, according to the Bureau's continuous monitoring strategy, requiring the most frequent periodic assessments. OIG found that almost half (2,718 of 6,240) of the instances of controls[5] had not been assessed within the last 2 years. In some cases, the Bureau had not assessed its highest risk controls in 5 years, or since 2012.

The lack of ongoing assessments indicate that the risk-based decisions made by Bureau management—to authorize these systems to operate while continuous monitoring was not occurring—were based on inaccurate information about what assessment activities had been, and would be, performed to assure their secure operation. Thus, Bureau management and staff had an insufficient basis for understanding the effectiveness of security controls protecting vital Bureau operations.

[4] The Bureau divides the NIST 800-53 revision 4 security controls into multiple security requirements referred to as *control steps derived from assessment steps in NIST SP 800-53A revision 4*. NIST, April 2013. *Security and Privacy Controls for Federal Information Systems and Organizations: Joint Task Force Transformation Initiatives*, NIST SP 800-53, rev. 4. Gaithersburg, MD: NIST (NIST SP 800-53, Rev. 4).

[5] Census systems have multiple instances of a control requirement because they are made up of multiple subsystems that may, depending on their function, have to implement the control requirement for each subsystem.

OIG discussed these issues with Bureau senior IT security officials in June 2017. Bureau management took action by developing a continuous monitoring plan for conducting periodic assessments of security controls. In February 2018, OIG followed-up on the Bureau's implementation of the plan and found that its ongoing periodic assessments have largely adhered to the plan's schedule. In addition, the Bureau updated its continuous monitoring policy to require management notification of deviations from the continuous monitoring schedule. However, because the policy revision requires self-reporting, there is less assurance that issues will be reported.

Recommendation

OIG recommends that the Bureau CIO 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.

II. Authorizing Officials Lacked Information About Significant Cybersecurity Risks

In 2017, OIG reviewed the reports that Bureau management used to assess the cybersecurity risks of five systems. Although these reports indicated cybersecurity risks were relatively low, OIG's review found that, at the time the systems were authorized to operate, security control implementations had not been described or assessed, leaving little to no assurance that a large portion of the controls protecting these systems were adequately implemented. OIG also conducted a general review of Bureau-wide practices for assessing security controls and found that the Bureau did not consistently follow required procedures. As a result, RMPS reports used by management to authorize systems to operate did not accurately portray cybersecurity risks.

A. Security control implementations had not been described or assessed

NIST Special Publication 800-53[6] describes a catalog of security and privacy controls for federal information systems and organizations designed to help protect them from an increasingly diverse landscape of cyber threats. The publication provides guidance on tailoring these controls to address the security requirements for protecting an organization's specific missions, business operations, technologies, environments and applications. Although the Bureau had identified the required security controls for these five systems, in many cases the Bureau had not described how it actually implemented the controls in its systems. In addition, the Bureau had not assessed the effectiveness of many other controls, either at all or within the previous 2 years as minimally required. Across the five systems, OIG found that the Bureau had both described in RMPS and adequately assessed only 18 percent of required security controls (see table 2 below).

[6] NIST SP 800-53, Rev. 4.

Table 2. Descriptions and Assessments of Security Controls for Sampled Systems

System	CEN01	CEN02	CEN03	CEN011	CEN016	Overall
Security Control Instances:	9,417	1,397	5,933	6,219	3,430	26,396
Controls not described	48%	44%	65%	51%	43%	52%
Controls described but not assessed	28%	21%	17%	22%	16%	22%
Controls described but not assessed within last 2 years	12%	2%	4%	3%	15%	8%
Controls described and assessed within last 2 years	12%	33%	14%	24%	26%	18%

Source: OIG analysis of data from RMPS used as the basis for these systems to be authorized to operate in July 2016.

Specifically, OIG found the following:

- ***Roughly half of security controls were not described in RMPS.*** OIG found that a significant number of implementations of security control requirements in RMPS were not described at all. Instead, they were left blank (e.g., up to 65 percent in one system; see table 2). The majority of the blank descriptions were associated with requirements introduced by NIST SP 800-53 revision 4. Under the Federal Information Security Modernization Act of 2014 (FISMA), the Bureau was required to describe how it would implement these control requirements by January 2015.[7] While the Bureau had identified in RMPS which new security control requirements applied to these systems, it failed to describe how it would meet the requirements. Thus, there was no basis to assess the effectiveness of the controls—or even to understand how or if they were implemented.

- ***Some security controls were described but had never been assessed.*** Without an assessment, there is no assurance that a security control is implemented and effective. A large number of required control implementations described in RMPS (up to 28 percent in one system) had never been validated with an assessment (see table 2).

- ***Other security controls had not been assessed in over 2 years.*** A portion of security controls described in RMPS (up to 15 percent for one system) had not been assessed within the previous 2 years (see table 2). As stated in finding I, Bureau policy requires

[7] Department of Commerce, September 2014. *Information Technology Security Program Policy*.

that the time between security control assessments should not exceed 2 years. According to NIST,

> [a]s the time period between current and previous assessments increases, the credibility and utility of the previous assessment results decrease. This is primarily due to the fact that the information system or the environment in which the information system operates is more likely to change with the passage of time, possibly invalidating the original conditions or assumptions on which the previous assessment was based.[8]

B. Security control assessments were insufficient to ensure the validity, credibility, and utility of the results

OIG's broader look at Bureau-wide security control assessments found that the Bureau had not consistently assessed controls according to its required procedures.[9] The assessment of security controls serves as a validation that controls are operating as intended; results of these assessments inform management about the risks of operating a system. The Bureau's procedures require that control assessments and results be recorded in RMPS. However, OIG found that there was often little or no assurance in the validity, credibility, and utility of the assessments recorded in RMPS.

Specifically, we found the following:

- ***One-third of security control assessments lacked documentation to support their validity, as required by the Bureau's standard.*** The Bureau's procedures require assessors to record the results of their assessments in RMPS, along with an indication of whether the control passed or failed and a description of how they made that determination. OIG analyzed all system-specific assessment results documented in RMPS as of March 2017 and found that 6,678 out of 20,120 assessments lacked a description of how assessors made their determinations, giving little or no assurance that the results were valid.
- ***Date inconsistencies in RMPS lessen the credibility and utility of assessments.*** OIG found that in 32,113 out of 117,518 assessments (27 percent), affecting all 29 systems we reviewed, there was evidence that the assessment had been performed significantly earlier than the date recorded in RMPS (e.g., the assessment statement indicated an assessment occurred in 2014, but the assessment date recorded in RMPS indicated it had taken place in 2016).[10] Thus, much of the information management used as the basis for risk decisions was not current and therefore of less utility than depicted in RMPS.

[8] NIST SP 800-53A, rev. 4, 21.

[9] Census Bureau, December 2016. *New System Security Control Assessment Standard Operating Procedure,* Washington, DC: Census Bureau.

[10] OIG did not fully enumerate each instance, because assessments were recorded in a variety of formats—which limited the use of automated methods to identify each occurrence.

C. RMPS risk scores were not reflective of actual risks, but the Bureau has since made progress with standardized reports

The RMPS-generated reports for senior managers did not convey the lack of descriptions of security control implementations and assessments. As a result, management believed it had an understanding of the risks—when, in reality, the actual risks to the system were largely concealed.

In June 2017, OIG briefed IT security staff on the identified issues and they immediately began to develop corrective action plans. In February 2018, OIG reviewed the Bureau's progress and found that it had standardized RMPS risk reports presented to management. Generally, OIG found that current risk reports are more representative of the risks associated with operating IT systems because they incorporate more of the information that was lacking in the prior reports we reviewed. A comparison of the old and updated reports presents a different picture of the cybersecurity risks to operating these systems (see table 3, below, for a comparison of the previous risk scores reported to current risk scores reported for the same systems).

Table 3. Comparison of Total System Risk[a] as Reported to Authorizing Officials

	Risk Score Reported	
System	**July 2016**	**February 2018**
CEN 01	4.91%	31.88%
CEN 02	2.75%	28.28%
CEN 03	.98%	23.89%
CEN 011	1.57%	25.22%
CEN 016	2.81%	27.45%

Source: RMPS scores provided by the Census Bureau.

[a] These figures represent the total system risk for five systems as reported via RMPS to Bureau management in July 2016 and February 2018. Total system risk is calculated by RMPS and represents the risks identified out of the total potential risks that could be identified for a particular system. In July 2016 the Bureau's acceptable risk threshold was 5 percent. However, the Bureau has since abandoned the use of this threshold.

OIG also found that the Bureau is in the process of developing new security control assessment procedures to address some of the issues we identified.

OIG concludes that Bureau management—including authorizing officials—was not sufficiently aware of the actual security posture of its systems. Further, the automation afforded by RMPS allows for quick identification and quantification of controls that have not been described, assessment results that are incomplete, and the age of assessments. Despite the availability of this information within RMPS, the Bureau did not fully utilize the automated capabilities in RMPS to identify these issues.

Recommendations

OIG recommends that the Bureau CIO do the following:

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.

III. The Bureau Did Not Effectively Manage Common Controls

If a system relies on a common control, a security control that protects multiple systems, then the relying system "inherits" that control. The Bureau uses RMPS to identify the inheritance of common controls across its enterprise. In March 2017, OIG 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. When control inheritance is not properly understood (and recorded within RMPS), the risks to operating a system may be over- or under-stated. Further, ineffective common control assessments can lead system owners across the enterprise to believe their systems are protected when they are not.

Specifically, OIG found the following:

- ***Common auditing and monitoring controls were not accurately represented within RMPS.*** OIG, in reviewing 65 subsystems that were reportedly inheriting enterprise auditing and monitoring controls, assessed whether (a) these controls were correctly inherited within RMPS and (b) the subsystems were actually being monitored. OIG found that 27 of these subsystems were incorrectly identified as inheriting this control (i.e., RMPS indicated they were being monitored, but no monitoring services were actually being provided). In addition, OIG identified a subset of components (417 total, such as Windows or Linux servers) within 13 subsystems that were not sending logs to the monitoring service. As a result, the incorrect depiction of inheritance of these controls within RMPS skewed the risks reported to management. Further, these common controls had either never been assessed or had not been assessed within the prescribed 2-year period.

- ***Common secure configuration standards were not met, but RMPS reports indicated systems were compliant.*** RMPS showed that secure configuration standards were implemented on 34 subsystems. The Bureau developed required secure configuration standards to identify what settings, services, or features should be disabled, enabled, or limited on IT products (e.g, operating systems, databases) to best protect its systems. OIG selected and reviewed one subsystem with a large number of components and found that 80 percent of them (2,899 out of 3,614) were not compliant with the required configuration standards, with the level of compliance varying by component. For example, configurations for use of compliant cryptography were not consistently configured correctly. RMPS reports did not identify the risks associated with these vulnerabilities because the Bureau's assessment results indicated this control was fully implemented. However, OIG found that the actual assessment statements, which should describe how these assessment results were determined, were blank.

- ***Common account management controls were inconsistently implemented.*** RMPS indicated that the Bureau's common account management process was implemented. OIG reviewed 23 privileged user accounts[11] to determine whether the Bureau followed its required account management process that includes initiating a ticket to create, change, or delete an account and found that the Bureau
    - had followed the required process for only 2 accounts,
    - partially followed the required process for 9 accounts, and
    - did not follow any part of the process for the remaining 12.

  Furthermore, OIG found that the Bureau's past assessments of account management controls were not sufficient to determine that the actual process had been followed. This was because the assessments either relied on document review, rather than a system account review, or did not collect enough evidence to demonstrate that the controls were implemented. Because this common control can potentially impact many Bureau systems, greater rigor should be applied to assessing it so system owners that inherit these controls can have sufficient confidence that user accounts have appropriate access to their systems.

- ***Inheritance of controls from enterprise desktop services was not supported.*** OIG attempted to validate 11 specific security control requirements that RMPS indicated enterprise desktop services[12] provided for 17 subsystems. Bureau managers told OIG that, in fact, the subsystems inherited 9 of the 11 security controls from enterprise desktop services and that its support for this assertion was "decisions made by the prior Census CIO." However, management could not

[11] Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions.

[12] A component of Census system CEN17, Desktop-Laptop Computing Environment Windows Devices.

produce documentation to support how the subsystems actually inherited the 9 controls.

Further, OIG identified basic incongruities that suggested that some subsystems could not inherit controls from enterprise desktop services. For example, a subsystem of network switches would not inherit account login controls from enterprise desktop services, which is intended for Windows operating system environments. Documenting security decisions would provide transparency and greater assurance that underlying assumptions, constraints, and rationale supporting those decisions are consistently applied. NIST specifically emphasizes that

> Documenting significant risk management decisions in the security control selection process is imperative so that authorizing officials can have access to the necessary information to make informed authorization decisions for organizational information systems. Without such information, the understanding, assumptions, constraints, and rationale supporting those risk management decisions will, in all likelihood, not be available when the state of the information systems or environments of operation change, and the original risk decisions are revisited.[13]

In June 2017, OIG briefed IT security staff on the issues we identified. As a result, they developed an action plan to revalidate the accuracy of the inheritance of common controls within RMPS. In February 2018, OIG reviewed the actions taken and found that the Bureau had instituted an enhanced change management process for common control inheritance. However, the Bureau still had not corrected almost half of the inaccuracies that OIG had previously identified.

Recommendations

OIG recommends that the Bureau CIO do the following:

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.

[13] NIST SP 800-53, Rev. 4, 42.

Summary of Agency Response and OIG Comments

In response to our draft report, the Bureau concurred with our findings and recommendations. The Bureau stated that it "collects and tracks a more granular level of detail than most other federal agencies, which enables the Census Bureau. . . to be more transparent and objective." The Bureau also provided explanatory comments for each finding and requested changes to the report.

We have summarized more details of the response below, along with our comments. The Bureau's complete response to our draft report is in appendix B.

OIG Comments:

We are pleased that the Bureau concurs with our findings and recommendations. While the Bureau's RMF implementation tool did have significant granularity of information, our report generally reviewed the Bureau's actions to provide accurate and complete security information needed to assess risk. Our findings are a result of inadequacies in those needed activities. We have considered each of the Bureau's requested changes but do not agree that any are supportable or relevant and have therefore not made changes in the final report.

On finding I:

The Bureau asked that we consider that its policy requiring continuous monitoring of controls every 2 years was more frequent than the federal requirement of every 3 years and asked that we adjust the percentages in table 1 to represent a 3-year cycle rather than a 2-year. The Bureau also asked that we note that they have put into place a continuous monitoring strategy more in line with federal requirements.

OIG response:

The NIST Risk Management Framework requires agencies to conduct ongoing security control assessments in accordance with the organization-defined monitoring strategy.[14] Department policy gives operating units the option to develop their own process for assessing controls as long as they establish the timeframes for monitoring controls. The Bureau's policy clearly stated that assessments were to occur within a 2-year period, which was the basis for our assessment.

[14] *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach*, Special Publication 800-37, Rev. 1. June 5, 2014. Gaithersburg, MD: NIST. RMF Step 6, Task 6-2.

On finding II.A:

The Bureau requested that OIG note that the Bureau had made a resource-based decision not to migrate fully to NIST SP 800-53 revision 4 and instead migrate fully to revision 5 when issued by NIST. The Bureau also requested that OIG note that delaying the move to revision 4 did not significantly change its systems' overall security posture "other than non-compliance with policy."

OIG response:

The Bureau made the decision not to comply fully with NIST SP 800-53 revision 4 on November 14, 2017, more than 4 years after revision 4's publication. Non-compliance was a longstanding issue. As highlighted in the finding, the Bureau failed to describe how more than half of the required security controls for the systems we assessed were actually implemented. As such, there was no basis to understand whether controls existed or how well controls actually provided protection. This does affect the security posture beyond the simple assertion of non-compliance.

On finding II.B:

The Bureau requested that OIG acknowledge that the Bureau did not use missing assessment data as a factor for risk scores. Instead, the Bureau stated that missing or inaccurate data was the result of errors from a migration of data from a previous report format, and that the Bureau's decision-making was based on the previous reports, which "contained the correct date and determination information."

OIG response:

As stated in the introduction of this report, the effectiveness of the Bureau's risk management program depended heavily on the accuracy and integrity of the information maintained within RMPS. The Bureau's response notes that within RMPS, assessment data was either missing or inaccurate.

We found that there was often little or no assurance in the validity, credibility, and utility of the assessments recorded in RMPS. While assessment results do not factor into the risk score, they do provide assurance that control assessments occurred. The artifacts that we assessed within the scope of this audit—Excel spreadsheets that the Bureau used to support 2016 authorization decisions—contained records that had blank assessment statements or incorrect dates.

On finding II.C:

The Bureau asked that OIG reconsider the use of the word "conceal," arguing, "It was never the intent to 'conceal' pending risk," yet also noting that reports did not include pending and inherited risks. (Note: the Bureau considers controls with an unknown implementation status as "Pending Risk.") The Bureau also claimed that a 5 percent acceptable risk threshold was not accurate and not used to inform management decisions.

OIG response:

Our use of the word "conceal" accurately conveys the resulting effects of the deficiencies in the Bureau's risk reports we reviewed. With respect to the 5 percent risk threshold, each of the systems' risk reports used to support authorization decisions included a 5 percent risk threshold indicator. In addition, as recently as 2018, risk reports generated by RMPS include an appendix that defines the current Enterprise Risk Threshold as 5 percent of the system's Potential Risk.

On Finding III:

The Bureau requested that OIG state that control tailoring was initially correct but because of a lack of continuous monitoring and ongoing validation, "the documentation became outdated." The Bureaus also asked that OIG note that while there was no formal decision memo to tailor controls for its enterprise desktop services, "compensating controls and risk acceptance was formally approved, albeit not documented."

OIG response:

We cannot comment in the report about the initial state of the control tailoring because it was not assessed within the scope of our audit. Our review found that the tailoring was not correct, which the Bureau affirms in its response. Finally, as our report makes clear, documenting security decisions is needed to provide transparency and greater assurance that underlying assumptions, constraints, and rationale supporting decisions are consistently applied. The importance of documentation is further emphasized in NIST SP 800-53, as cited in our report.

Appendix A: Objective, Scope, and Methodology

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.

OIG reviewed controls significant within the context of the audit objective and applied a comprehensive methodology to evaluate the security posture of five moderate-impact Bureau systems judgmentally selected for review. Also, OIG reviewed Bureau policies and procedures related to IT security and the Bureau's implementation of the RMF—and interviewed Bureau officials, including IT security staff and management. In addition, OIG reviewed and assessed system security-related artifacts relevant to the time of authorization to operate for the five selected systems described in table A-1.

Table A-1. Census Bureau Systems Selected for Review

System Name	Brief Description	Date of System Authorization
CEN01—Data Communications	Serves as the medium to interconnect the various Bureau information systems that are deployed.	July 28, 2016
CEN02—LENEL	An electronic access control system that controls physical access via Homeland Security Presidential Directive 12 compliant Personal Identification Verification card access.	July 13, 2016
CEN03—Economic Programming Division Applications	Supports the Bureau's Economic Programs Directorate, which is responsible for statistical programs that measure and profile U.S. businesses and government organizations.	July 28, 2016
CEN11—Demographic Census, Surveys, and Special Processing	Includes applications that provide users with the ability to develop, collect, analyze, model and disseminate demographic data.	July 18, 2016
CEN16—Network Services	Consists of servers that are primarily managed by the Computer Services Division to support the Bureau's mission to collect U.S. statistical data.	July 28, 2016

Source: OIG analysis of Bureau system documentation.

OIG briefed Bureau IT security officials on preliminary findings in June 2017. In response to this briefing, the Bureau developed corrective action plans to begin to address some of the issues that OIG initially identified. Over summer and fall of 2017, the OIG audit team focused on competing its mandatory FISMA audit, returning to this audit work in 2018.

To assess actions taken to correct issues identified during audit fieldwork, OIG reviewed updated policies and procedures, assessment schedules, and updated risk reports generated by RMPS as of February 2018.

Further, OIG reviewed the Bureau's compliance with the following applicable internal controls, provisions of law, regulation, and mandatory guidance:

- The Federal Information Security Modernization Act of 2014
- IT Security Program Policy, U.S. Department of Commerce, introduced by the Chief Information Officer on September 12, 2014, and applicable Commerce Information Technology Requirements (CITR):
    - CITR-016, *Vulnerability Scanning and Patch Management*
    - CITR-017, *Security Configuration Checklist Program*
    - CITR-019, *Risk Management Framework (RMF)*
- NIST Federal Information Processing Standards Publications:
    - 199, *Standards for Security Categorization of Federal Information and Information Systems*
    - 200, *Minimum Security Requirements for Federal Information and Information Systems*
- NIST Special Publications:
    - 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
    - 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
    - 800-53A, Rev. 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations, Building Effective Assessment Plans*

OIG analyzed computer-processed data produced by RMPS. To assess data, OIG performed analysis, looking for missing data, data outside valid timeframes, and data completeness. Issues that OIG identified as a result of this analysis are detailed in the findings of this report.

Fieldwork was conducted from January 2017 to March 2018 at Department headquarters in Washington, DC, and Bureau offices in Suitland, Maryland. OIG performed this audit under the authority of the Inspector General Act of 1978, as amended, 5 U.S.C. App., and Department Organization Order 10-13, dated April 26, 2013, and in accordance with generally accepted government auditing standards. Those standards require that OIG plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and

conclusions based on the audit objectives. OIG believes that the evidence obtained provides a reasonable basis for the findings and conclusions, based on the audit objectives.

Appendix B: Agency Response

SEP 2 0 2018

MEMORANDUM FOR: Frederick J. Meny, Jr.
Assistant Inspector General for Audit
and Evaluation (Acting)
Office of Inspector General

THROUGH: Ron S. Jarmin
Performing the Non-Exclusive Functions
and Duties of the Director
U.S. Census Bureau

FROM: Kevin B. Smith
Associate Director for Information Technology
and Chief Information Officer
U.S. Census Bureau

Subject: Response to OIG Draft Report: *The Census Bureau Must Improve Its Implementation of the Risk Management Framework*

This memo responds to the OIG Draft Report: *The Census Bureau Must Improve Its Implementation of the Risk Management Framework*. The U.S. Census Bureau appreciates the Office of Inspector General's (OIG's) review of the effectiveness of our Risk Management Framework (RMF) methodology and the underlying system supporting it. The Census Bureau concurs with the findings and, as the OIG mentions, has already implemented resolutions for many of the identified findings.

While concurring with the recommendations, it is important to recognize that the Census Bureau collects and tracks a more granular level of detail than most other federal agencies, which enables the Census Bureau and the underlying system supporting our implementation of the RMF to be more transparent and objective. The greater availability of detailed data provides visibility into each individual component and enables senior management to make the most informed decisions. This additional detail also enabled the OIG, by its own admission, to conduct a more detailed assessment of the Census Bureau's RMF program, methodology and security posture.

The Census Bureau strives to continuously improve our methodology and processes and welcomes the OIG's recommendations to improve the use of data to more efficiently inform senior management of risks and enable them to more effectively manage enterprise risk.

Response to Specific Sections of the Draft Report

Objective, Findings and Recommendations

The Census Bureau has no comments on this section.

I. The Bureau Had Not Continuously Monitored Critical Security Controls and Failed to Document the Resulting Risks

The Census Bureau requests the OIG consider that the previously documented methodology requiring assessment of controls every two years was more frequent than the federal requirement of every three years. We request that OIG include in Table 1 the percentage of controls assessed within the three-year federal requirement.

The Census Bureau also requests that OIG recognize that, based upon an evaluation of time and resource constraints, the Census Bureau has now put in place a continuous monitoring strategy commensurate with available resources and more in line with federal mandates.

II. Authorizing Officials Lacked Information About Significant Cybersecurity Risks

A. *Security Control Implementations had not been described or assessed.*

The Census Bureau requests the OIG note that the Census Bureau made a resource-based decision to complete only a portion of the migration to Revision 4 of National Institute of Standards and Technology (NIST) Special Publication 800-53 and non-implemented Plan of Action & Milestones (POA&M) items. The Census Bureau does plan to fully implement Revision 5 when it becomes available.

The Census Bureau also requests that the OIG consider indicating that the delay in moving from SP 800-53 Revision 3 to SP 800-53 Revision 4 does not significantly change the overall security posture of the Census Bureau other than non-compliance with policy. Per NIST, many of the changes (in Revision 4) were driven by particular cyber issues and challenges rather than a blanket update to the entire security control catalog.

B. *Security control assessments were insufficient to ensure the validity, credibility and usability of the results.*

The Census Bureau requests the OIG acknowledge that the missing assessment data was not used by the Census Bureau as a factor into the computation of the risk score or used in decision-making.

The Census Bureau also requests that the OIG note that the missing or inaccurate data was the result of errors from a technical migration from a previous reporting format (Excel) to

the Risk Management Program System (RMPS). The Excel reports, not the RMPS, were used for decision-making and contained the correct date and determination information.

C. ***RMPS risk scores were not reflective of actual risks, but the Bureau has since made progress with standardized reports.***

The Census Bureau requests that the OIG reconsider using the word "conceal." The risk reports used by the previous Chief Information Officer (CIO) included accepted and residual risk, and not inherited and pending risk, in the final risk assessment analysis. When the current CIO arrived, the team recognized this deficiency. CIO risk reporting now includes all accepted, residual, pending, and inherited risks. It was never the intent to "conceal" pending risk. The Census Bureau requests that the final sentence of the first paragraph in this section be edited as follows: "As a result, while management believed it had an understanding of the risks—a portion of the risks to the system were omitted from the RMPS report."

In Section C, the footnote for Table 3 references that the "Bureau's acceptable risk threshold was 5 percent." The Census Bureau requests Footnote A be removed from the report because it is not accurate. The stated 5 percent was never formalized in any Census Bureau policy, established as an acceptable risk threshold, or used to inform risk management decision-making.

III. The Bureau Did Not Effectively Manage Common Controls

The Census Bureau requests the OIG consider stating that control tailoring was initially correct. However, due to the previously cited lack of continuous monitoring, validation of common control implementation was not completed, and therefore documentation became outdated. Upon initial system documentation and authorization, inheritance was validated, however, ongoing validation was not included as part of the Information Security Continuous Monitoring (ISCM) process.

Regarding the reference that there was no formal decision memo documenting the decision to tailor the controls for enterprise desktop services, the Census Bureau requests the OIG to consider noting that the compensating controls and risk acceptance was formally approved, albeit not documented.

OIG Recommendations/Responses

Recommendation #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.

Response – *The Census Bureau agrees with this recommendation.* The Census Bureau established a corrective action plan to reinstate continuous monitoring which was completed in November 2017. In July 2018, the Census Bureau implemented monthly CIO Scorecards to provide continuous monitoring status to Authorizing Officials and System Owners.

The Census Bureau is transitioning from the RMPS to the commercial product, RSA Archer, to improve management of the Risk Management Framework. RSA Archer is capable of producing automated notifications to kick-off continuous monitoring processes and is configured to notify stakeholders when due dates are missed. The Census Bureau will leverage these automated reporting features to ensure senior management is aware of any deviations to the continuous monitoring process.

Recommendation #2 - Ensure that management is informed when risks are omitted from RMPS reports.

Response – *The Census Bureau agrees with this recommendation.* In July 2018, the Census Bureau incorporated pending risk into all tier reports and reviews it annually with key stakeholders of each report. Any further activity will be captured in a formal plan of action and milestones.

Recommendation #3 - Develop both manual and automated procedures to help ensure that completion descriptions of system security controls are entered into RMPS, reviewed, and approved as part of the system authorization process.

Response – *The Census Bureau agrees with this recommendation.* The Census Bureau will examine the ability in RSA Archer to include an integrity check of the system security plan and assessment information. Any further activity will be captured in a formal plan of action and milestones.

Recommendation #4 - Ensure that assessment procedures include provisions (both manual and automated) for quality control associated with the validation of security control assessments.

Response – *The Census Bureau agrees with this recommendation.* The Census Bureau will validate the current security control assessment

procedures to evaluate the effectiveness of the current quality assurance methods. Any further activity will be captured in a formal plan of action and milestones.

Recommendation #5 - Develop a strategy for periodically verifying the accuracy of common control inheritance within RMPS.

Response – *The Census Bureau agrees with this recommendation.* The Census Bureau will develop a formal plan of action and milestones to develop a strategy to verify the accuracy.

Recommendation #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.

Response – *The Census Bureau agrees with this recommendation.* The Census Bureau will develop a formal plan of action and milestones.

Recommendation #7 - Clearly document the rationale for common control decisions within RMPS.

Response – *The Census Bureau agrees with this recommendation.* The Census Bureau will develop a formal plan of action and milestones to create traceability between recipients and providers of common controls and rationale for the inheritance.

If you have any questions regarding this matter, please contact Kevin B. Smith, CIO, at 301-763-2117 or Ron Jarmin, Performing the Non-Exclusive Functions and Duties of the Director, at 301-763-1858.

cc: Rod Turk, Acting Chief Information Officer, Department of Commerce
Timothy P. Ruland, Chief Information Security Officer, Census Bureau
Jeffrey Jackson, Deputy Chief Information Security Officer, Census Bureau
Colleen Holzbach, Program Manager for Oversight Engagement, Census Bureau
Jean McKenzie, IT Security Audit Liaison, Census Bureau

011200072274