

Fundamental Security Safeguards Were Not In Place to Adequately Protect the IT Systems Supporting the 2020 Census

FINAL REPORT NO. OIG-21-018-A

JANUARY 7, 2021

FOR PUBLIC RELEASE



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



~~FOR OFFICIAL USE ONLY~~
~~Final Report Contains Information Marked~~
~~For Official Use Only~~

January 7, 2021

MEMORANDUM FOR: Dr. Steven Dillingham
Director
U.S. Census Bureau

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

SUBJECT: *Fundamental Security Safeguards Were Not In Place to Adequately
Protect the IT Systems Supporting the 2020 Census*
Final Report No. OIG-21-018-A

Attached is our final report on our audit of the U.S. Census Bureau's (the Bureau's) decennial information technology (IT) security measures. Our objective was to determine the effectiveness of security measures for select IT systems that support the 2020 decennial census.

We found the following:

- I. The Bureau's inadequate risk management program left significant risks present in decennial IT systems.
- II. The Bureau's Decennial security operations center lacked fundamental capabilities during periods of decennial census data collection.
- III. The Bureau inadequately managed its Active Directory that supports decennial census operations.
- IV. The Bureau had not fully enforced personal identity verification in accordance with federal and Department requirements.

Please note that portions of finding III on pages 10 and 11 of this final report have been labeled as For Official Use Only.

On November 16, 2020, we received the Bureau's response to our draft report. In response to our draft report, the Bureau concurred with our recommendations and described actions it has taken, or will take, to address them. We summarized the Bureau's response and provided our comments within the Summary of Agency Response and OIG Comments section of the final report. In addition, based on the Bureau's response, we made changes to the final report where

appropriate. The Bureau's complete formal response is included within the final report as appendix D.

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. This 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), with redaction of information that is For Official Use Only.

We appreciate the cooperation and courtesies extended to us by your staff during our audit. If you have any questions or concerns about this report, please contact me at (202) 482-1931 or Dr. Ping Sun, Director for IT Security, at (202) 482-6121.

Attachment

cc: André Mendes, Chief Information Officer
Kevin B. Smith, Chief Information Officer, Census Bureau
Colleen Holzbach, Program Manager for Oversight Engagement, Census Bureau
Corey J. Kane, Audit Liaison, Census Bureau
Kemi A. Williams, Program Analyst for Oversight Engagement, Census Bureau
Ken White, Audit Liaison, OUS/EA
Deborah Stempowski, Assistant Director for Decennial Census Programs (Operations & Schedule Management), Census Bureau
Michael Thieme, Assistant Director for Decennial Census Programs (Systems & Contracts), Census Bureau
Joselyn Bingham, Audit Liaison, Office of the Chief Information Officer
MaryAnn Mausser, Audit Liaison, Office of the Secretary



Report in Brief

January 7, 2021

Background

The U.S. Census Bureau (the Bureau) is responsible for conducting a decennial census as mandated by the United States Constitution to ensure an accurate count of the U.S. population. Data collected during a decennial census are used to determine the number of seats each state will be apportioned in the U.S. House of Representatives, define congressional districts, and distribute billions of dollars in federal funds for infrastructure and public services, such as highways, hospitals, and schools.

During the 2020 decennial census (the 2020 Census), the Bureau used the Internet to collect sensitive data of U.S. individuals and businesses protected under Title 13 of the U.S. Code. These protected Title 13 data include PII (personally identifiable information), such as names, addresses (including GPS coordinates), dates of birth, and telephone numbers. The far-reaching consequences of altered, lost, or stolen Title 13 data emphasize the necessity to safeguard the Bureau information technology (IT) systems that support the 2020 Census.

Why We Did This Review

The objective of this audit was to determine the effectiveness of security measures for select IT systems that support the 2020 Census. Our audit scope included the Bureau's risk management program, security operations center (SOC) capabilities, security of Active Directory, and implementation of multi-factor authentication.

U.S. CENSUS BUREAU

Fundamental Security Safeguards Were Not In Place to Adequately Protect the IT Systems Supporting the 2020 Census

OIG-21-018-A

WHAT WE FOUND

We found that fundamental security safeguards were not in place to adequately protect the Bureau's IT systems supporting 2020 Census operations. Specifically, the Bureau's inadequate risk management program left significant risks present in decennial IT systems, some of which were identified in our previous audit report. We also found that the Bureau's Decennial SOC lacked fundamental capabilities during the 2018 End-to-End Census Test and address canvassing campaign, which included the collection of Title 13 protected data.

Furthermore, the Bureau inadequately managed its Active Directory that supports decennial operations by allowing excessive access rights and not properly managing user accounts. In addition, the Bureau had not enforced personal identity verification (PIV) in accordance with federal and Departmental requirements.

WHAT WE RECOMMEND

We recommend that the Director of the U.S. Census Bureau ensure that the Bureau's Chief Information Officer does the following:

1. Develop and adhere to risk acceptance policies and procedures in accordance with the National Institute of Standards and Technology risk management framework (NIST SP 800-37).
2. Reassess all instances of security risks on the decennial IT infrastructure that were accepted without mitigation and ensure correct actions are taken to minimize existing security risks.
3. Ensure critical SOC capabilities are in place and operating as intended by immediately verifying (a) the implementation and operation of a file level encryption for all required resources; (b) the implementation of a technical solution for data loss prevention is fully functional; and (c) the implementation and complete vulnerability scanning coverage of all required databases.
4. Regularly perform a thorough review of Active Directory configurations and ensure that all active accounts have the minimum access rights to fulfill operational requirements. Consider the feasibility of using specialized software tools to augment the Bureau's review of Active Directory configurations.
5. Prioritize the enforcement of PIV and other forms of multi-factor authentication (MFA) by (a) establishing a process to validate the enforcement of federal PIV requirements for all users accessing Bureau resources via government-owned computers and (b) regularly verifying that all privileged access to the Bureau network or its resources for contractors working on-site at the Bowie Computer Center or Bureau headquarters in Suitland, Maryland, is protected with MFA in accordance with federal and Department requirements.

Contents

Introduction	1
Objective, Findings, and Recommendations	2
I. The Bureau’s Inadequate Risk Management Program Left Significant Risks Present in Decennial IT Systems	2
Recommendations	6
II. The Bureau’s Decennial SOC Lacked Fundamental Capabilities During Periods of Decennial Census Data Collection	7
Recommendation	9
III. The Bureau Inadequately Managed Its Active Directory That Supports Decennial Census Operations	9
A. <i>The Bureau inadequately configured its Active Directory that allowed excessive access rights</i>	10
B. <i>The Bureau inadequately managed Active Directory accounts</i>	11
Recommendation	12
IV. The Bureau Had Not Fully Enforced PIV in Accordance With Federal and Department Requirements	12
Recommendation	13
Summary of Agency Response and OIG Comments	14
Appendix A: Objective, Scope, and Methodology	17
Appendix B: Risk Response Strategies	19
Appendix C: Required Controls in Blanket-Risk-Acceptance Documents	20
Appendix D: Agency Response	21

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

The U.S. Census Bureau (the Bureau) is responsible for conducting a decennial census as mandated by the United States Constitution to ensure an accurate count of the U.S. population.¹ Data collected during a decennial census are used to determine the number of seats each state will be apportioned in the U.S. House of Representatives, define congressional districts, and distribute billions of dollars in federal funds for infrastructure and public services, such as highways, hospitals, and schools.

During the 2020 decennial census (the 2020 Census), the Bureau used the Internet to collect sensitive data of U.S. individuals and businesses protected under Title 13 of the U.S. Code. These protected Title 13 data include PII (personally identifiable information), such as names, addresses (including GPS coordinates), dates of birth, and telephone numbers. The far-reaching consequences of altered, lost, or stolen Title 13 data emphasize the necessity to safeguard the Bureau information technology (IT) systems that support the 2020 Census.

¹ U.S. Const. art. I, § 2.

Objective, Findings, and Recommendations

The objective of this audit was to determine the effectiveness of security measures for select IT systems that support the 2020 Census. Our audit scope included the Bureau's risk management program, security operations center (SOC) capabilities, security of Active Directory, and implementation of multi-factor authentication. We conducted our technical analysis during 2020 Census preparations before the internet self-response had begun. Appendix A provides a more detailed description of our audit objective, scope, and methodology.

We found that fundamental security safeguards were not in place to adequately protect the Bureau's IT systems supporting 2020 Census operations. Specifically, the Bureau's inadequate risk management program left significant risks present in decennial IT systems, some of which were identified in our previous audit report.² We also found that the Bureau's Decennial SOC lacked fundamental capabilities during the 2018 End-to-End Census Test and address canvassing campaign, which included the collection of Title 13 protected data.

Furthermore, the Bureau inadequately managed its Active Directory that supports decennial operations by allowing excessive access rights and not properly managing user accounts. In addition, the Bureau had not enforced personal identity verification (PIV) in accordance with federal and Departmental requirements.

These identified deficiencies increase the likelihood of adverse effects on the confidentiality, integrity, and availability of the Title 13 data collected and processed by the Bureau's IT systems. Throughout this audit, we worked with Bureau system administrators, security staff, and management so that the security issues we identified could be immediately addressed. This coordination allowed the Bureau to remediate some of these issues before the conclusion of our audit.

I. The Bureau's Inadequate Risk Management Program Left Significant Risks Present in Decennial IT Systems

All federal agencies are required to adhere to the National Institute of Standards and Technology (NIST) risk management framework (RMF)³—a methodical and pragmatic approach for cost-effective and risk-based decisions regarding IT security resource allocation to support mission and business functions. By executing the tasks outlined in the RMF, management obtains assurance that risks are mitigated to acceptable levels. Risks that are identified while conducting risk management activities can be responded to in one of

² U.S. Department of Commerce Office of Inspector General, June 19, 2019. *The Census Bureau Must Correct Fundamental Cloud Security Deficiencies in Order to Better Safeguard the 2020 Decennial Census*, OIG-19-015-A. Washington, DC: DOC OIG. Available online at <https://www.oig.doc.gov/OIGPublications/OIG-19-015-A.pdf> (accessed September 1, 2020).

³ DOC National Institute of Standards and Technology, December 2018. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Special Publication (SP) 800-37, Rev. 2. Gaithersburg, MD: DOC NIST.

four ways: accepted, avoided, mitigated, or transferred.⁴ Risks that are determined to require mitigation and cannot be promptly resolved are tracked through to mitigation with a plan of action and milestones (POA&M)⁵ document. Risks that are accepted are required to be accompanied with

- (1) an explanation of circumstance justifying foregoing the implementation of the control;
- (2) a description of all compensating controls reducing the risks associated with the inability to implement the control; and
- (3) a description of any residual risk introduced as a result of not implementing the control.⁶

As part of our audit, we analyzed all accepted risk instances⁷ (6,629) for the decennial IT infrastructure,⁸ and found that the Bureau identified risks associated with security control deficiencies during final preparations for the 2020 Census. Due to a compressed schedule during 2020 Census preparations, Bureau leadership accepted large amounts of risk without adequate justification or evidence of mitigation.

Significant risks were present when system authorization was granted

In a September 2019 memo, the Bureau's then-acting Chief of the Office of Information Security and then-acting Chief Privacy Officer reported that significant risks were present in the decennial IT infrastructure which "could have serious adverse impacts to the U.S. Census Bureau."⁹ Those risks included the following:

- Unauthorized and high-risk software installations
- Excessive cloud virtual machine (VM) instances
- Incomplete and outdated inventory
- Configuration management processes not being followed
- Inadequate incident response plans

⁴ For more information on risk treatment, see appendix B.

⁵ A POA&M is a document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

⁶ DOC, June 2019. *U.S. Department of Commerce Information Technology Security Baseline Policy (ITSBP)*, Ver. 1.0. Washington, DC: DOC, sect. 2.

⁷ Instance can be defined in this report as an individual observation of identified risk via a security control deficiency.

⁸ The accepted risk instances that were analyzed were those recorded from February 2017 through August 2019. At the time of our audit fieldwork, this included all instances. For more information on our methodology, see appendix A.

⁹ U.S. Census Bureau, September 20, 2019. *Risk Evaluation of Assessment Findings for 2020 Census Infrastructure (CEN08 2020 Census Infrastructure)*. Washington, DC: Census Bureau.

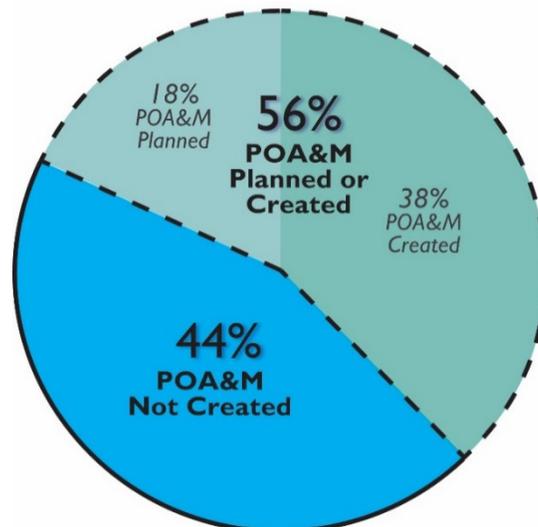
- No backup solution or disaster recovery policy and procedures

Despite these significant risks, the Bureau renewed the decennial IT infrastructure's authorization to operate (ATO)¹⁰ during 2020 Census preparations. Additionally, our previous audit on the Bureau's cloud-based IT systems supporting the decennial census also reported on inventory, configuration management, and backup/disaster recovery issues.¹¹ The Bureau planned to implement our recommendations from that report by the end of 2019, but, as of issuance of this report, all recommendations remain unimplemented. During this audit, we continued to observe issues related to inventory and configuration management.

Considerable risk was accepted without adequate justification

Our analysis found that system security officials had determined 56 percent of the accepted risk instances required mitigation, as indicated by the Bureau's assignment of POA&Ms. Specifically, we found 38 percent (2,539 out of 6,629) of the instances had an associated POA&M, and 18 percent (1,166 out of 6,629) were determined to need POA&Ms but they were not created. The remaining 44 percent (2,924 out of 6,629) of accepted risk instances were not assigned and were not planned for a POA&M. However, Bureau leadership ultimately decided to address all 6,629 instances of risk with blanket-risk-acceptance. These numbers are further illustrated in figure 1.

Figure 1. Accepted Risk Instances POA&M Breakdown



Source: Created by OIG based on analysis of Bureau risk documentation

¹⁰ NIST defines an ATO as the “official management decision given by a senior official to authorize operation of a system or the common controls inherited by designated organizations systems and to explicitly accept the risk to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls.” See definition available online at https://csrc.nist.gov/glossary/term/Security_Authorization (accessed September 1, 2020).

¹¹ OIG-19-015-A.

Bureau leadership approved blanket-risk-acceptance documents that contained inadequate justification for risk acceptance and no evidence of mitigation. In fact, each blanket-risk-acceptance document repeated the following statement:

Due to compressed development, testing, and production schedules required to meet operational deadlines, the program was unable to provide artifacts showing implementation of all controls prior to receiving an Authorization To Operate (ATO), resulting in a number of findings/POAMs. Due to ongoing schedule and resource constraints and competing operational priorities, and with an understanding of the findings/POAM's low level of criticality and residual risk, the TI¹² seeks Risk Acceptance for the findings/POAMs listed below.

The Bureau consistently claimed low levels of quantified risk to justify the use of blanket-risk-acceptance documents. The Bureau relied upon output from its Risk Management Program System to quantify the risk for each of the NIST security control families.¹³ However, as we reported in 2018,¹⁴ the Bureau's Risk Management Program System generated reports used by management to authorize systems to operate did not accurately portray cybersecurity risks. The Bureau planned to implement our recommendations from that report by the end of 2019, but as of issuance of this report, all remain unimplemented. This leads us to question the accuracy of the Bureau's quantified risk within the decennial IT infrastructure for which acceptance was granted.

Significantly, the blanket-risk-acceptance documents were used to accept risks associated with the majority of the required security controls for the decennial IT infrastructure (see appendix C). Specifically, the Bureau created a blanket-risk-acceptance document for 13 of the 17 NIST security control families, which justified the closure of hundreds of POA&Ms. Among these control families, Bureau leadership accepted the risk of identified security deficiencies for 64 percent (102 out of 159) of

¹² *TI* is an abbreviation for "technical integrator," which consists of contracted companies supporting the Census Bureau.

¹³ The NIST security control catalog contains a robust collection of security controls categorized by family. For more information, see DOC NIST, April 2013. *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53 Rev. 4. Gaithersburg, MD: DOC NIST, app. F. Available online at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf> (accessed September 2, 2020).

¹⁴ DOC OIG, October 30, 2018. *The Census Bureau Must Improve Its Implementation of the Risk Management Framework*, OIG-19-002-A. Washington, DC: DOC OIG. Available online at https://www.oig.doc.gov/OIGPublications/2018-10-30_Census_RMF_Final_Audit_Report.pdf (accessed September 2, 2020).

the system's required security controls,¹⁵ despite the blanket-risk acceptance documents providing no evidence of the implementation of these controls.¹⁶

Moreover, we found the blanket-risk-acceptance documents listed unimplemented security tools as compensating capabilities for multiple control deficiencies and risks. Specifically, we found an encryption tool and data loss prevention tool were referenced for the Media Protection control family, which is discussed in further detail within finding II of this report. We also found a behavioral analytics tool was referenced for the Access Control control family, which the Bureau procured but never implemented. These tools were not in place to protect sensitive data, yet they were relied upon to compensate for identified risks. Due to the large number of compensating security tools listed in the blanket-risk-acceptance documents, we did not verify all of them during our audit.

The absence of risk acceptance policies and procedures contributed to the Bureau's deficient risk acceptance activities. Ultimately, the inadequate risk management processes carried out by the Bureau did not provide assurance that accepted risks were mitigated to acceptable levels and allowed a significant number of risks to remain within the systems supporting the 2020 Census. The integrity of census data is crucial. If population numbers were manipulated, representation in the House of Representatives and federal money distribution could be disproportionately distributed. Proper risk management is paramount to ensure the adequate protection of sensitive data.

Recommendations

We recommend that the Director of the U.S. Census Bureau ensure that the Bureau's Chief Information Officer does the following:

1. Develop and adhere to risk acceptance policies and procedures in accordance with the NIST RMF (NIST SP 800-37).
2. Reassess all instances of security risks on the decennial IT infrastructure that were accepted without mitigation and ensure correct actions are taken to minimize existing security risks.

¹⁵ NIST states, "FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, is a mandatory federal standard developed by NIST in response to [the Federal Information Security Management Act of 2002]. To comply with the federal standard, organizations first determine the security category of their information system in accordance with FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, derive the information system impact level from the security category in accordance with FIPS 200, and then apply the appropriately tailored set of baseline security controls in NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*." See SP 800-53 Rev. 4, p. vi. NIST SP 800-53 and the Department's *ITSBP* define a baseline of 159 controls for moderate-impact systems.

¹⁶ Among these accepted risks, some were associated with the fundamental security capabilities identified in findings II, III, and IV of this report.

II. The Bureau's Decennial SOC Lacked Fundamental Capabilities During Periods of Decennial Census Data Collection

The 2020 Census depends on its Decennial SOC (referred to hereafter as “SOC”) to provide protection of data and network resources from internal and external threats. To do so, the SOC was tasked with implementing a selected set of security tools to carry out needed capabilities for IT systems supporting the 2020 Census. However, we found that the SOC had not fully implemented several security capabilities that the Bureau deemed necessary to secure Title 13 data. Not only were these capabilities considered best practice, but Bureau leadership designated some of them to satisfy required security controls to protect information systems within the Bureau's network boundary.

During an interview with Bureau leadership in charge of the 2020 Census, SOC officials stated that several essential security capabilities for the 2020 Census were not in place. However, Bureau web resources had been storing sensitive data collected during the 2018 End-to-End Census Test in Rhode Island and its critical address canvassing campaign. We found the capabilities responsible for file level encryption, data loss prevention (DLP), and database vulnerability scanning were not operating as intended to protect sensitive Title 13 data.

Encryption of sensitive data

According to system security documentation, the file level encryption¹⁷ solution was selected to satisfy NIST requirements for cryptographic protection and protection of information at rest for all moderate-impact systems. However, we found that the capability was not in-place during collection of Title 13 data during the 2018 End-to-End Census Test and address canvassing campaign. Although the Bureau did implement disk level encryption, this form of encryption only mitigates risk associated with physical threats such as theft or loss. Disk level encryption provides no protection against unauthorized access to files once someone gains access to the system.

The file level encryption solution required client software to be functional. Despite SOC documentation indicating that the file level encryption tool was operational, we found the necessary client software was not installed on all intended systems in October 2019. In fact, up until January 20, 2020, the SOC's file level encryption capability was providing coverage for less than 40 percent of devices that the Bureau had determined required the tool. Additionally, when a majority of supported systems had client software installed on them, we found that the security configuration policies used to enforce its capabilities had not been configured to actually enforce security policies. This configuration made the tool unable to perform its full functionality of restricting access to sensitive data by using file level encryption.

¹⁷ File level encryption is a method of encrypting individual files and directories.

Data loss prevention (DLP)

According to system documentation, the Bureau intended to implement a DLP¹⁸ solution to provide the SOC with the ability to track data across the network and automatically block any intentional or unintentional data exfiltration attempts. The DLP capability was also intended to provide media access control capabilities, and guard against removable media, such as portable USB devices. However, during the aforementioned October 2019 interview with SOC leadership, we found that these DLP capabilities were not in-place.

During our audit, we reviewed SOC documentation stating that the DLP tool was operational. However, we found that the tool was inadequately configured to provide an effective DLP solution. During interviews with SOC engineers, we discovered that the tool had not been configured to perform an essential function: to automatically block data from leaving the network. Instead, the DLP capability had only been configured to create an alert when it detected data being exfiltrated from the network, which would be insufficient to prevent sensitive data from being obtained by malicious actors.

Without these vital capabilities in-place, data collected and stored in the decennial census environment was not only vulnerable to data exfiltration in clear text, but it could not be tracked or blocked as it moved across the decennial IT infrastructure.

Database vulnerability scanning

Specialized database vulnerability scanning¹⁹ was the SOC's solution to manage vulnerabilities, privileges, and user activity on databases within the decennial IT infrastructure. However, during the 2018 End-to-End Census Test and address canvassing campaign this capability was not in place. Once the tool was operational, we found that it was performing credentialed scans on 88 percent (346 out of 395) of cloud databases and 60 percent (241 out of 399) of databases hosted within a Bureau data center as of February 2020. Non-credentialed scanning is limited because it does not allow the tool to have trusted access to the database, as opposed to credentialed scanning which provides a more in-depth inspection by providing the tool administrative access to the databases. By not conducting in-depth vulnerability scans using a specialized database scanner, the Bureau was unable to address potential vulnerabilities from known exploits.

After briefing the Bureau on our observations at the conclusion of our audit, the Bureau provided artifacts showing Decennial SOC file-level encryption, DLP, and database vulnerability scanning capabilities were deployed and configured by March 2020. However, prior to March, the Bureau had little assurance that these capabilities were in place or adequately configured to safeguard Title 13 data. When questioned about the delayed

¹⁸ DLP is a capability that detects potential data breaches or ex-filtration transmissions and prevents them by monitoring, detecting, and blocking sensitive data while in use, in motion, and at rest.

¹⁹ Database vulnerability scanning identifies weaknesses, misconfigurations, and known vulnerabilities in databases.

implementation of essential SOC capabilities, Bureau officials attributed it to errors in design architecture associated with the initial implementation solution for each of the tools.

Recommendation

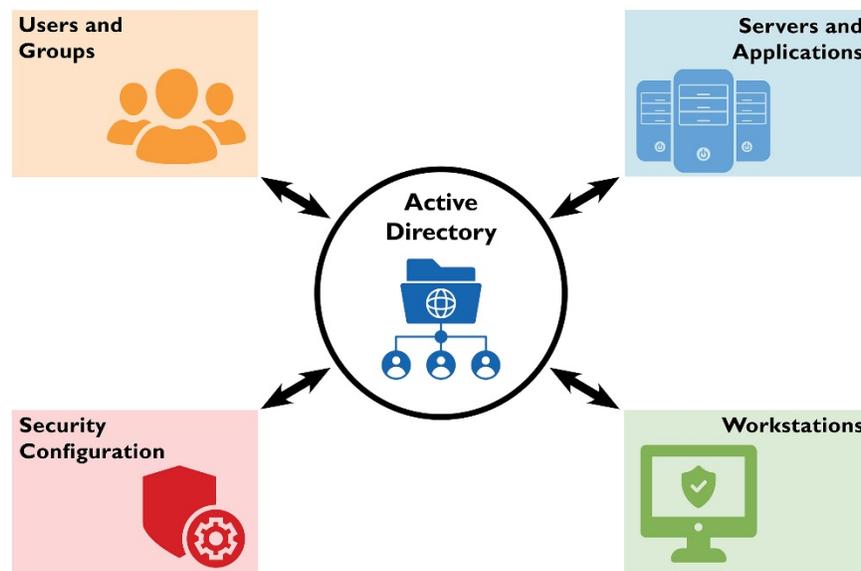
We recommend that the Director of the U.S. Census Bureau ensure that the Bureau's Chief Information Officer does the following:

3. Ensure critical SOC capabilities are in place and operating as intended by immediately verifying (a) the implementation and operation of a file level encryption for all required resources; (b) the implementation of a technical solution for DLP is fully functional; and (c) the implementation and complete vulnerability scanning coverage of all required databases.

III. The Bureau Inadequately Managed Its Active Directory That Supports Decennial Census Operations

Active Directory is a critical component of the Bureau's decennial census IT infrastructure. It maintains a logical structure—known as a *domain*—to manage all network resources within the domain. If managed properly, Active Directory provides a secure, centralized means to manage network users, workstations, servers, printers, databases, and system configurations. (See figure 2.)

Figure 2. The Concept of Active Directory



Source: OIG

Due to the nature of its role, Active Directory holds sensitive information such as users' credentials and network topologies, making it a prime target for cyberattacks. To support the 2020 Census, the Bureau deployed a specific Active Directory instance. We used a specialized tool to assess the Active Directory instance, and found that the Bureau

inadequately configured it to allow excessive access rights and inadequately managed its accounts.

A. *The Bureau inadequately configured its Active Directory that allowed excessive access rights*

One of the primary Active Directory roles is to manage user accounts' access permissions. To facilitate this management, Active Directory user accounts are commonly organized into separate groups with varying permission levels. To comply with the least privilege security principle, a NIST control requirement,²⁰ each group must be given access permissions only to relevant function areas required by users' roles and responsibilities. We found that the Bureau configured four user groups to have unneeded local administrator rights on hundreds of servers. Specifically,

- one group containing 639 users had local administrator rights on 179 servers;
- one group containing 120 users had local administrator rights on 172 servers;
- one group containing 38 users had local administrator rights on 260 servers; and
- one group containing 23 users had local administrator rights on 172 servers.

Because local administrative rights allow remote code execution, these rights can be exploited by attackers for lateral movement from one compromised server to another on the Bureau's network. In addition, attackers can abuse these rights to gather user credentials (username and password), impersonate other users, and disable security products installed on servers such as anti-virus software.

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

21

22

In addition, one server was found to be configured with unconstrained delegation. *Unconstrained delegation* is a Microsoft Windows feature that can be configured on a server. Once configured, it allows the server to acquire all rights of a user who logged into it, therefore user rights are delegated to the server. If an attacker compromises a server with unconstrained delegation, this feature can be abused to steal credentials (usernames and passwords) and potentially gain further unauthorized access to other

²⁰ NIST SP 800-53, Rev 4.

²¹ FOR OFFICIAL USE ONLY

²² FOR OFFICIAL USE ONLY

servers. To limit this risk, unconstrained delegation should only be configured when operationally necessary following the security principle of least privilege.

Attackers can leverage a combination of excessive access rights, **FOR OFFICIAL USE ONLY**, and unconstrained delegation to gain unauthorized access to the Bureau's servers supporting the decennial census and thus undermine confidentiality, integrity, and availability of critical data and applications.

B. The Bureau inadequately managed Active Directory accounts

The Bureau has two types of user accounts: (1) ordinary accounts for regular purposes, such as email and office work, and (2) privileged accounts for administrative functions.²³ Privileged user accounts are placed in administrative groups that have specific access rights able to perform administrative functions. Ordinary and privileged accounts should be properly separated and, therefore, administrative groups must not have any ordinary user accounts. However, we found several administrative groups that contained many ordinary user accounts. This gave privileged rights to these ordinary accounts that should not have been allowed. Specifically, we found 106 instances of ordinary users' accounts in three administrator groups.

Inadequate separation of user accounts allowed ordinary user accounts to perform administrative functions such as changing other users' passwords or assigning users to other Active Directory groups (and therefore modifying their access rights). Using a separate privileged account for administrative functions adds an extra layer of defense against cyberattacks. For example, when a user becomes a victim of a phishing attack, the user's ordinary account becomes compromised and the attacker assumes all of the user's rights. When an ordinary account has rights to perform administrative functions, it would allow an attacker to use these rights and potentially gain further access to systems and networks.

In addition, the Bureau did not disable or remove Active Directory inactive users in a timely manner as required by the Department's policy.²⁴ We found the following:

- Ten users that never logged in. After we notified the Bureau, it took action to remove these users.
- Eight users that had not logged in for more than 90 days.
- One user's password had not been changed in 11 months.

Keeping unnecessary inactive accounts increases the attack surface and the risk of system compromise.

²³ Examples of administrative functions are resetting passwords of other users or changing their group membership and therefore modifying access rights.

²⁴ *DOC Information Technology Security Program Policy* required users to be disabled after 60 days of inactivity and that passwords are changed every 90 days.

The reason for the deficiencies is that the Bureau did not perform adequate reviews of Active Directory. The Bureau conducted several reviews of Active Directory via a vendor contract, but the reviews were high-level and did not identify any of the weaknesses discussed in this finding. Once we identified these weaknesses and informed the Bureau, it took prompt action to remediate them.

Recommendation

We recommend that the Director of the U.S. Census Bureau ensure that the Bureau's Chief Information Officer does the following:

4. Regularly perform a thorough review of Active Directory configurations and ensure that all active accounts have the minimum access rights to fulfill operational requirements. Consider the feasibility of using specialized software tools to augment the Bureau's review of Active Directory configurations.

IV. The Bureau Had Not Fully Enforced PIV in Accordance With Federal and Department Requirements

The Bureau did not enforce federal requirements to use a PIV credential for contractors accessing Bureau resources via government-owned computers.²⁵ Federal requirements mandate a PIV card for physical and logical access to federally controlled information systems. The Bureau was not compliant with this requirement until after we discovered and notified the Bureau that PIV was not being fully enforced, which we discovered during an interview with contractors who had administrator access to sensitive Bureau systems.

Despite the federal mandate to require the use of PIV for federal employees and contractors by October 2005, the Bureau had still not implemented a technical solution to enforce PIV use until February 2020. In response to our request for evidence of PIV enforcement, a Bureau official provided artifacts that indicated the Bureau had just completed PIV enforcement as recently as February 5, 2020. In its response, the Bureau stated that it had incorporated the federal policy requiring the use of PIV cards to access the Bureau computer network into its *Acceptable Use Policy* in 2014. However, the Bureau stated that it did not begin implementing a technical policy to enforce the federal requirement throughout the Bureau until April 2019, with a target completion date of January 31, 2020.

We identified several reasons why the Bureau had not enforced PIV in accordance with federal and Department requirements.²⁶ According to a senior security official in the

²⁵ Homeland Security Presidential Directive-12 requires, to the maximum extent practicable, use of PIV for logical access to federally controlled information systems since October 2005. See U.S. Department of Homeland Security, August 27, 2004. *Policies for a Common Identification Standard for Federal Employees and Contractors*, HSPD 12. Washington, DC: DHS. Available online at <https://www.dhs.gov/homeland-security-presidential-directive-12> (accessed September 2, 2020).

²⁶ The *U.S. Department of Commerce Information Technology Security Baseline Policy* requires multi-factor authentication (MFA) for access to privileged accounts.

Program Management Office on the Technical Integration team, the Bureau had not enforced PIV for contractors because field office badging systems were not ready. However, according to the Bureau official whose office was responsible for applying the Active Directory enforcement of PIV, it took from April 2019 until February 2020 to enforce PIV across the Bureau because of other priorities. While the Bureau was behind schedule and competing priorities may have prevented it from focusing on PIV during final preparations for the 2020 Census, it is unclear why the Bureau had not enforced PIV prior to these preparations. In fact, we reported on a similar issue in our 2016 audit report²⁷ where we found the Bureau had not implemented multi-factor authentication for privileged users on PII systems—an issue the Bureau had planned to remediate by 2017.

The Bureau had not enforced PIV during collection of sensitive Title 13 data during the 2018 End-to-End Census Test and address canvassing campaign. The privileged access by contractors included administrative access to servers and applications that supported 2020 Census preparations. By not utilizing multi-factor authentication (MFA)²⁸ to protect privileged access to the network and critical resources that facilitated 2020 Census preparations, the Bureau incurred greater risk of cyberattack. For example, MFA could reduce the likelihood of user account exploitation using stolen usernames and passwords and help prevent unauthorized privilege escalation. Without the implementation of required MFA security controls, privileged accounts were more vulnerable to attackers who may attempt to exploit or disrupt the 2020 Census.

Recommendation

We recommend that the Director of the U.S. Census Bureau ensure that the Bureau's Chief Information Officer does the following:

5. Prioritize the enforcement of PIV and other forms of MFA by (a) establishing a process to validate the enforcement of federal PIV requirements for all users accessing Bureau resources via government-owned computers and (b) regularly verifying that all privileged access to the Bureau network or its resources for contractors working on-site at the Bowie Computer Center or Bureau headquarters in Suitland, Maryland, is protected with MFA in accordance with federal and Department requirements.

²⁷ DOC OIG, August 4, 2016. *Review of IT Security Policies, Procedures, Practices, and Capabilities in Accordance with the Cybersecurity Act of 2015*, OIG-16-040-A. Washington, DC: DOC OIG. Available online at <https://www.oig.doc.gov/OIGPublications/OIG-16-040-A.pdf> (accessed September 30, 2020).

²⁸ *Multi-factor authentication* (or *MFA*) is a method of authentication that requires the use of two or more pieces of evidence—their credentials—before a user is allowed access to a system. Their credentials fall into any of these three categories: (1) something they know (like a password or PIN), (2) something they have (like a smart card), or (3) something they are (like a fingerprint). Credentials must come from two different categories to enhance security—thus, entering two different passwords would not be considered multi-factor. (See <https://www.nist.gov/itl/tig/back-basics-multi-factor-authentication> [accessed September 4, 2020].) MFA helps protect a user's account from an attacker who has compromised the account's credentials, like a username and password.

Summary of Agency Response and OIG Comments

On November 16, 2020, we received the Bureau's response to our draft report. In its response, the Bureau concurred with our recommendations and described actions it has taken, or will take, to address them. We have summarized the Bureau's response and provided our comments below. In addition, based on the Bureau's response, we made changes to the final report where appropriate. The Bureau's complete formal response is included within this final report as appendix D.

We are pleased that the Bureau generally concurs with our recommendations, and look forward to reviewing its proposed audit action plan.

Introduction

The Bureau expressed generally that the content of our report does not reflect its security posture during the 2020 Census (i.e., March 9, 2020–October 15, 2020).

OIG response. This audit was to determine the effectiveness of security measures for select IT systems that support the 2020 Census at the time of our fieldwork, not the security posture of the entire 2020 Census operation. Our initial findings were observed during 2020 Census preparations before the internet self-response was conducted, which allowed the Bureau to implement corrective actions to address some of the issues we identified during our fieldwork. We have noted these corrective actions in the report. Appendix A provides a more detailed description of our audit objective, scope, and methodology.

The Bureau asserted that “there have been no incidents or loss or compromise of data” during the 2020 Census and asked us to include such a statement in our report.

OIG response. Our audit scope included the Bureau's risk management program, SOC capabilities, security of Active Directory, and implementation of multi-factor authentication. We did not assess the effectiveness of the Bureau's capability to identify and respond to potential security incidents related to the 2020 Census, or whether data was compromised. Therefore, we cannot make statements on the matter. However, we recently initiated an audit of the Bureau's incident response process,²⁹ and will present the outcome of this audit when completed.

Objective, Findings, and Recommendations

The Bureau requested that we include language that clearly defines the timelines of the overall decennial operation with specific dates for internet self-response and supporting operations.

²⁹ DOC OIG, November 12, 2020. *Audit of the U.S. Census Bureau's Incident Response Process (#2021-391)*. Washington, DC: DOC OIG. Available online at <https://www.oig.doc.gov/OIGPublications/Audit-of-the-U.S.-Census-Bureau's-Incident-Response-Process.pdf> (accessed November 30, 2020).

OIG response. We modified the use of “periods of decennial data collection” to the more specific “2018 End-to-End Census Test in Rhode Island and its critical address canvassing campaign” in the final report.

Section I

The Bureau stated that our findings in Section I neglected the authority held by agency authorizing officials to make a risk determination on behalf of the agency, and asked that we replace the terminology “blanket-accepted” with the term “accepted” throughout the report.

OIG response. We fully recognize that the Bureau has flexibility to implement its risk management policies and procedures within the boundaries of Department policies and procedures. As noted in the report, the Department ITSBP requires that any accepted risk instances related to required security control deficiencies be accompanied with (1) an explanation of circumstance justifying foregoing the implementation of the control; (2) a description of all compensating controls reducing the risks associated with the inability to implement the control; and (3) a description of any residual risk introduced as a result of not implementing the control. As stated in the report, the Bureau was not in compliance with the Department’s policy when accepting security risks.

We modified the use of “blanket-accepted” to “accepted” in the final report.

The Bureau stated that it provided us with risk acceptance policies and procedures, and that we were not consistent in characterizing its risk management policies and procedures.

OIG response. The last paragraph of finding I discusses the absence of *risk acceptance* policies and procedures—a subset of *risk management*. We requested the Bureau’s risk acceptance policies and procedures and were informed that the Bureau did not possess them.

Section II

The Bureau asked that finding II be updated to accurately reflect SOC capabilities on March 9, 2020—the time at which digital nationwide decennial data collection began. Additionally, the Bureau requested that we define the period during which the audit was conducted, and the point in time at which census systems went “live” and began processing citizen data. The response also commented on the implementation details related to SOC tools discussed in the report.

OIG response. We believe this report adequately reflects SOC capabilities during our audit. Specifically, the timeframe and scope of our audit were included in appendix A of the draft report. The two data collection periods—the 2018 End-to-End Census Test in Rhode Island and address canvassing campaign—were also specified in the introduction section of finding II in the report. We also have added clarification to ensure the reader understands the scope of our audit work.

Section III

The Bureau stated that it conducted several reviews of its Active Directory via a contract with Microsoft. In parallel, the Bureau ensured a proactive assessment posture by running regular BloodHound assessments on the TI domain beginning November 7, 2019.

OIG response. The statement regarding the Bureau utilizing BloodHound starting in November 7 factually contradicted our observations and the Bureau's own actions. First, in November 2019, we informed the Bureau of our intent to use the open-source tool BloodHound to assess its Active Directory and started coordinating this activity with the Bureau. On November 8, 2019, a Decennial Contracts Execution Office official expressed concerns in using the tool and stated that running BloodHound would require following the Bureau's change control request process. Additionally, on February 25 and March 10, 2020, the Bureau reported that it had remediated technical issues we had identified using BloodHound. Second, when we inquired in March 2020 about any Active Directory assessments conducted by the Bureau, the Bureau's response did not include the use of BloodHound, but instead only included Microsoft assessments.

Appendix A: Objective, Scope, and Methodology

Our audit objective was to determine the effectiveness of security measures for select IT systems that support the 2020 Census.

To do so, we

- reviewed system-related artifacts, including policy and procedures, planning documents, and security control documentation;
- interviewed Bureau officials, including system owners, system administrators, IT security and operations staff, and management;
- assessed the Bureau's Active Directory configuration using specialized open-source assessment tools and techniques; and
- performed analysis on the entire universe of 6,629 accepted risk instances for the Decennial system of systems where practical, such as when performing trend analysis or categorization.

We reviewed internal security controls significant within the context of our audit objective and employed a comprehensive methodology to evaluate the security posture of the Bureau's CEN08TI System, TI SOC, and TI Active Directory.

We reviewed the implementation status of fundamental security controls defined in NIST SP 800-53, Rev. 4, including security assessment and authorization, incident response, media protection, access control, configuration management, identification and authentication, and program management.

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

- The Federal Information Security Modernization Act of 2014
- The *U.S. Department of Commerce Information Technology Security Baseline Policy (ITSBP)*
- NIST Special Publications:
 - 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
 - 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*

We also used industry best practices as criteria for the review and testing of proper Active Directory configuration.

We collected computer-generated data directly from the Bureau's Active Directory. We verified this data by interviewing appropriate Bureau officials and provided them the data to eliminate the possibility of false positive results. We determined that the data were sufficiently reliable for the purposes of this report.

We conducted our review from October 24, 2019, through July 16, 2020, under the authority of the Inspector General Act of 1978, as amended (5 U.S.C. App.), and Department Organization Order 10-13, April 26, 2013. We conducted our technical analysis during 2020 Census preparations before the internet self-response had begun. We performed our fieldwork at Department headquarters in Washington, D.C.; Census Bureau headquarters in Suitland, Maryland; and a contractor site in Greenbelt, Maryland.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix B: Risk Response Strategies

NIST SP 800-39³⁰ identifies the following four risk response options:

Risk Acceptance: The organization explicitly understands and accepts the risk to its operations and assets, individuals, other organizations, and the nation (reflecting the organization's risk tolerance). Acceptance is made in accordance with the organization's risk management strategy.

Risk Avoidance: The organization does not start or continue the activity that presents the risk. This is the only risk response option that completely eliminates the risk.

Risk Mitigation: The organization reduces the negative effect of a risk by implementing security controls.

Risk Transfer or Sharing: The organization shifts the risk responsibility or liability, in whole (transfer) or in part (sharing), to another party.

³⁰ DOC NIST, March 2011. *Managing Information Security Risk: Organization, Mission, and Information System View*, SP 800-39. Gaithersburg, MD: DOC NIST.

Appendix C: Required Controls in Blanket-Risk-Acceptance Documents

ID	Control Family ^a	Number of Controls	Percentage
AC	Access Control	15/17	88%
AU	Audit and Accountability	11/11	100%
CM	Configuration Management	11/11	100%
IA	Identification & Authentication	8/8	100%
IR	Incident Response	4/8	50%
MA	Maintenance	6/6	100%
MP	Media Protection	5/7	71%
PL	Planning	3/4	75%
RA	Risk Assessment	1/4	25%
CA	Security Assessment & Authorization	2/7	29%
SC	System & Communications Protection	17/19	89%
SI	System & Information Integrity	10/11	91%
SA	System & Services Acquisition	9/9	100%

Source: Created by OIG based on analysis of Bureau risk documentation

^a The following four NIST control families are not included in the table because an associated blanket-risk-acceptance document was not found: (1) Awareness & Training, (2) Contingency Planning, (3) Physical & Environmental Protection, and (4) Personnel Security.

Appendix D: Agency Response



UNITED STATES DEPARTMENT OF COMMERCE
Economics and Statistics Administration
U.S. Census Bureau
Office of the Director
Washington, DC 20233-0001

November 16, 2020

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

FROM: Steven D. Dillingham 
Director
U.S. Census Bureau

SUBJECT: Response to *OIG Report: Fundamental Security Safeguards Were Not in Place to Adequately Protect the IT Systems Supporting the 2020 Census*

The draft report of the Office of Inspector General (OIG) entitled *Fundamental Security Safeguards Were Not in Place to Adequately Protect the IT Systems Supporting the 2020 Census* finds **no instances of loss or compromise of data collected on Census IT systems**. In fact, all Census IT systems and data collected during the 2020 Census remain safe and secure, and the 2020 Census self-response systems successfully supported over 100 million responses without any down time or security incidents. At the end of the data collection period, the 2020 Census was able to account for 99.98 percent of all addresses in the United States. We believe the fact that there have been no incidents or loss or compromise of data in what has been a census resulting in one of the highest national address resolution rates in history warrants mentioning in the opening portions of OIG's report.

While the Census Bureau appreciates the work of OIG generally in providing recommendations that have helped the Census Bureau prepare for a successful Decennial Census, we must note that the gaps identified in this report were addressed **prior to collecting and processing 2020 Census responses from the public**. We ask that OIG recognize these successful efforts of our dedicated career staff in its report, particularly by revising the report to reflect the following facts.

This memorandum includes detailed responses and requested changes to language in the draft report. Implementation of these changes will ensure clarity and more closely reflect the status of the security safeguards in place to protect the 2020 decennial census ahead of digital decennial data collection.

The Census Bureau strives to maintain and continuously improve cybersecurity methodologies and processes. Leading up to the 2020 Census, the Bureau welcomed several external organizations—including the Department of Homeland Security, the Government Accountability Office (GAO), our OIG, and private sector experts like Mitre and FireEye—to assess our environment and make recommendations for any relevant and timely improvements. The Census Bureau's measure of success has always centered on our cyber readiness ahead of the March 9, 2020, soft launch of the internet self-response web site.



census.gov

The Bureau provided artifacts between November 2019 and February 2020 to OIG that demonstrated the current status of IT systems, prior to their use in support of the decennial census. However, this snapshot should not be taken to represent a complete and accurate picture of the cybersecurity posture of the Bureau at the start of decennial data collection via self-response. Neither does it represent the progress achieved by the Bureau prior to launching internet self-response. Planned work remaining at the time of the audit was completed before soft launching the decennial self-response operation on March 9, 2020. All decennial IT systems supporting self-response and call center operations were fully authorized and secured at or above federally mandated security levels to protect citizen data prior to that date.

Lastly, in response to findings related to Title 13 data collected during the 2019 Address Canvassing operation, the Bureau would like to differentiate between data collected and stored on government owned devices—such as those used by staff in the Field—and the data collected publicly from citizens. The Bureau takes seriously the charge to protect all data entrusted to us, but would like to highlight the additional layers of security that exist by default when data is collected and stored on government equipment versus the layers of security that must be in place to protect data from the general public via the internet.

Responses to Specific Sections of the Draft Report

Objective, Findings and Recommendations

The Census Bureau requests that OIG include language that clearly defines the timelines of the overall decennial operation with specific dates for internet self-response and supporting operations under review, since technology and cybersecurity are the focus of this report. Specifically, please clarify that digital response collection, processing, and storage occurred between March 09, 2020 and October 15, 2020. While the full decennial operation and timeline began in January 2020, the IT systems assessed in this audit were not in production until March 2020 when self-response was launched nationwide. The broad term “periods of decennial data collection” (p. 2, 5) may cause the reader to mistakenly equate overall 2020 Census timelines with IT system readiness timelines.

- i. Requested revisions to Section I: “Bureau’s Inadequate Risk Management Program Left Significant Risks Present in Decennial IT Systems”
 - a. In line with the Census Bureau’s request above regarding the opening portions of OIG’s report, we request that the title of this section be amended to reflect the fact that **there were no instances of loss or compromise of data collected on Census IT systems.**
 - b. The Census Bureau asks that OIG replace the terminology “blanket-accepted” with the term “accepted” throughout this report. The term “blanket-accepted” is not defined by NIST 800-37 rev2 and could imply that no reviews of risk were associated with the assessment, and subsequent authorization, of systems supporting the decennial census

occurred. The Census Bureau has presented evidence to the OIG describing its risk acceptance process and the events that took place in support of this process. The Bureau's policies and processes align with NIST 800-37 rev2, which states that "The organization determines the level of formality for the process of communicating and acknowledging continued risk acceptance by the authorizing official (AO)." By this standard, the Census Bureau followed the NIST recommendations for reviewing and accepting risks associated with systems supporting the decennial systems. The Census Bureau also elected to conduct penetration testing and tabletop activities to test the resiliency of security systems in place to protect sensitive decennial data.

- c. The Bureau asks that the OIG define "instances" (p. 4) as used in this report to ensure understanding and avoid undue alarm. The 6,629 instances of risk analyzed in this report refer to specific test steps included in granular review and assessment of security controls as part of Census processes. As stated in previous responses, the Bureau collects and tracks a more granular level of detail than most federal agencies, ensuring transparency and objectivity. This detailed information provides enhanced awareness for senior management, enabling them to make the most informed decisions possible.
- d. Finally, the Census Bureau has made notable progress in addressing the recommendations provided by the OIG in response to the 2017 Report "The Census Bureau Must Improve Its Implementation of the Risk Management Framework," (p. 5). The Bureau has implemented quality controls, automated processes and procedures, increased visibility of risks at the executive level, and prepared systems for compliance ahead of the NIST 800-53 Rev 5 publication.

A. OIG's contention that significant risks were present when system authorization was granted is inaccurate.

OIG's characterization of identified and managed risks as "significant" (p. 3) directly conflicts with risk management principles, and neglects the authority held by agency authorizing officials to consider all relevant context, mitigations, and business requirements in order to make a true risk determination on behalf of the agency. The Census Bureau provided artifacts of the continuous monitoring and ongoing authorization process to demonstrate the effectiveness of the process. In alignment with the OIG's 2017 report on the Bureau's Risk Management Framework (RMF) Recommendation 2, "Ensure that management is informed when risks are omitted from RMPS reports," staff presented the highest risk scenario to the AO. With this knowledge in hand, the AO evaluated and accepted the risks.

Following Census's ongoing authorization process, AOs again granted authorization for these systems in July 2020. All outstanding risks noted in the 2019 memo had been addressed or

subsumed into the authorization process, demonstrating the Census Bureau's commitment to continually improving the security posture as expeditiously as possible given constraints to staff, schedule, and budget.

Lastly, the Bureau has completed all activities recommended by the OIG in the report "The Census Bureau Must Correct Fundamental Cloud Security Deficiencies in Order to Better Safeguard the 2020 Decennial Census" and is in the process of formal close-out.

B. OIG's contention that considerable risk was "blanket-accepted" without adequate justification fails to take into account key facts.

Again, the Census Bureau requests that OIG avoid the term "blanket-accepted" (p. 4). The term fails to convey a notable finding, since bulk management of compliance related requirements is common in many organizations. In addition, Census risk acceptance procedures follow NIST requirements, while risk management broadly falls within both business and technical AOs authority. Elsewhere in the report, the OIG notes that the Bureau had generally provided justification as part of the agency's risk acceptance process but held the opinion that it lacked consistency and rigor in the process. Removal of the term "blanket-accepted" conveys more clearly to the reader that, while there was risk, Bureau staff did complete due diligence in reviewing and managing risks and related impacts before choosing to move forward with acceptance in a business-driven manner.

As stated in the Bureau's response to the 2017 RMF audit conducted by the OIG, the Bureau made changes in July 2018 to its Risk Management Profiling System (RMPS), incorporating Pending/Projected Risk into all tier reports and presentations to AOs. RMPS reports are configured to require all types of risk to be displayed on all reports, including the ability to visualize additional details when reviewing Pending/Projected Risk and Assessed Risk. Risk scores, while important, are just one input into risk management decisions. Ultimately, a System Owner must decide, based on their intimate knowledge of a system, whether to move forward with authorization.

Risks were identified, accepted with justification, and managed at the discretion of the Census Bureau. The Census Bureau followed its documented risk acceptance processes in addressing and accepting risk, which allows for risk acceptance based on Bureau defined justification or remediation. The policy is in alignment with NIST 800-37 Rev 2, and allows for the AO to accept risk based on the following:

- Technology - Inability to implement requirements due to vendor limitations/capabilities
- Operational/Environment- Inability to implement controls because of location/configuration of systems, or due to needs mission requirements
- Policy/Regulatory - Inability to implement Federal/Agency/Bureau requirements/mandates

- based on mission/operational necessity
- Scalability - Inability to scale out systems to meet requirements/mandates based on mission necessity (i.e. solution unable to handle all the interactions or requirements)
- Resource Constraints - Inability to increase resources to meet requirements/mandates (i.e. hiring additional staff to close out POAMs; timeline challenges)

Whether tracked as a Plan of Action and Milestones (POA&M) or a Risk Acceptance, the Census Bureau manages and addresses risks as part of our ongoing authorization process. The Census Bureau AO maintains visibility of risks and sets priorities based on mission critical factors on a yearly basis. This approach, along with the commitment of countless dedicated professionals, led to an incontrovertibly successful 2020 Census operation that leveraged internet self-response for the first time in U.S. history.

Regarding specific language used, the Bureau has two requests: 1) In the second to last paragraph of this section (p. 6), the OIG writes, "It is possible that additional referenced capabilities were not implemented fully or at all." The Census Bureau requests that this sentence be removed from the report, as it is both suggestive and unsubstantiated. 2) In the concluding paragraph of this section (p. 6), the OIG moves from characterizing the Census Bureau's risk management practices as inadequate to using the phrase, "The absence of." While the Bureau does not agree with the assessment of our risk management process—and has presented evidence to the OIG to the contrary—the Bureau does ask that the OIG be consistent in their assessment of the processes and procedures being reviewed.

Finally, the Census Bureau asks that the OIG reconsider the placement of the statement, "The integrity of census data is crucial, because manipulated numbers could skew representation in the House of Representatives and federal money distribution," (p. 6). The Census Bureau recognizes the importance of the decennial census in guiding dissemination of federal funds and representation within the House of Representatives. The Bureau is concerned that the placement of this statement might inadvertently suggest to the reader that the security programs' deficiencies caused a direct impact on the fidelity of the results of the Census when (1) there is no evidence to that effect, and (2) the final numbers being developed to provide to the President, in addition to the effect of those numbers on funding distribution are the subject of numerous ongoing lawsuits against the Bureau, and the placement of such a statement in the report suggesting a manipulation of numbers where there is no evidence to support such a statement will only have an undue negative effect to the ongoing litigation .

The Bureau has worked closely with the GAO, Cybersecurity and Infrastructure Security Agency (CISA) cybersecurity experts and industry leading cybersecurity experts throughout decennial operations to review and evaluate all IT systems and has identified no evidence of compromise or

breach. Throughout the planning and execution of the decennial census, the Census Bureau has followed all federal guidance in conducting risk management activities. Our System Owners and Authorizing Officials have collaborated with system teams throughout this process and have made risk informed business decisions in order to protect the sensitive data entrusted to the Census Bureau accordingly.

II. Requested Revisions to Section II: “The Bureau’s Decennial Security Operations Center (SOC) Lacked Fundamental Capabilities During Periods of Decennial Census Data Collection”

A. *The Bureau asks that this finding be updated to accurately reflect SOC capabilities on March 9, 2020—the time at which digital nationwide decennial data collection began. Additionally, the Census Bureau requests the OIG define the period during which the audit was conducted, and the point in time at which Census systems went “live” and began processing citizen data. When the Census Bureau began internet self-response alongside operations to digitize previously collected paper data, the Decennial SOC was fully operational and capable of monitoring and responding to any potential security concerns. Census also conducted quarterly 2020 Program Management Reviews (PMRs); as part of these reviews Census communicated that March 9, 2020 was the start date for data collections. This information was publicly available and was previously communicated to the OIG.*

B. *Encryption of sensitive data*

Multiple encryption tools were in place during the timeframe for which evidence for this Audit was collected. We appreciate OIG’s support in protecting Bureau security by obfuscating tool names, however this has the effect of creating the impression that only one encryption tool was in place at the time. Census Bureau systems are supported by an encryption stack at both the file and “envelope” level, in line with the decennial encryption strategy and relevant FIPS accreditation procedures.

C. *Data loss prevention (DLP)*

The Census Bureau had previously implemented a host based DLP solution. However, while conducting performance and scalability testing, the solution did not meet Census Bureau standards for performance. As previously communicated to OIG, a network DLP solution was implemented in its place, with full coverage achieved prior to the start of decennial data collection.

D. *Database vulnerability scanning*

The Bureau uses multiple tools to conduct vulnerability scanning. On any given day, one of four different tools is scanning the Census environment based on a federally required 72-hour schedule. The Census Bureau has not captured any findings which would suggest that these tool sets were not in place and adequately scanning the environment.

III. Requested Revisions to Section III: “The Bureau Inadequately Managed Its Active Directory That Supports Decennial Census Operations”

A. *OIG’s assertion that the Bureau inadequately configured its Active Directory to allow excessive access rights is ambiguous and fails to take into account the Bureau’s security processes.*

The Bureau asks the OIG to define the term “excessive” (p. 10) in the context of the decennial census operation. This term is ambiguous and does not clearly convey a finding.

The Census Bureau followed its pre-defined process for staff to request regular and privileged accounts through our established Remedy process. Requests followed the appropriate review and approval layers, ensuring that only those with a need for enhanced privileges received access to such accounts. Given the scale and scope of software developed ahead of the 2020 Census, the Bureau granted access to and approved an accordant number of users in order to complete work as planned, including testing across multiple environments. The Bureau monitors accounts on a monthly basis using Bloodhound, and removes users as needed.

The Bureau also conducted several reviews of its Active Directory via a contract with Microsoft. In parallel, the Bureau ensured a proactive assessment posture by running regular Bloodhound assessments on the TI domain beginning November 7th, 2019. These assessments led the Census Bureau to begin pushing security recommendations and enabling generation of the data needed for the OIG to accomplish this specific review.

B. *OIG’s contention that the Bureau inadequately managed Active Directory accounts is incorrect.*

The Census Bureau runs regular reports utilizing Bloodhound and via contract with Microsoft. Inactive accounts are disabled when identified but may also be allowed to remain due to a small handful of exceptions, including human resource--related reasons. When weaknesses are identified they are remedied promptly.

IV. Requested Revisions to Section IV: “The Bureau Had Not Fully Enforced PIV in Accordance With Federal and Department Requirements”

As noted in the draft report, the Census Bureau issued an updated mandate to enforce PIV use for access to all government laptops and system maintainer devices as of February 2, 2020. Access to Decennial systems is restricted to Census Bureau devices, while administrative access is managed through the enterprise Active Directory instance. The Active Directory instance is set to enforce PIV, including multi-factor authentication using RSA Tokens.

[OIG Recommendations/Census Bureau Responses](#)

Recommendation 1. Develop and adhere to risk acceptance policies and procedures in accordance with the NIST RMF (NIST SP 800-37).

Response The Census Bureau concurs with the recommendation but maintains that we are in compliance.

The Census Bureau followed existing risk acceptance processes during authorization of the Decennial systems. The bureau also reviews lessons learned and adds additional detail and rigor to always strengthen and improve processes. The Bureau's continuous focus on risk management policies and processes ensures a strong security posture.

Unrelated to this recommendation, the Census Bureau has embarked on RMF refresh activities to strengthen and refine processes and policies by increasing the consumption and use of cyber threat intelligence to track active cyber threats and mitigate risk at an appropriate level.

Recommendation 2. Reassess all instances of security risks on the decennial IT infrastructure that were blanket-accepted without mitigation and ensure correct actions are taken to minimize existing security risks.

Response The Census Bureau concurs with the recommendation but maintains that we are in compliance.

Over the past year, as part of the Bureau's ongoing authorizations and continuous monitoring processes, the decennial systems were first assessed in July 2018, then reassessed and reauthorized as planned in July 2019 and July 2020. The Census Bureau conducts continuous monitoring on all decennial IT infrastructure and systems throughout their functional life until full decommission. The Census Bureau will continue to use risk acceptance and POA&Ms as appropriate, exercising risk management and mitigation strategies as directed by authorizing officials and based on available resources.

Recommendation 3. Ensure critical SOC capabilities are in-place and operating as intended by immediately verifying (a) the implementation and operation of a file level encryption for all required resources; (b) the implementation of a technical solution for DLP is fully functional; and (c) the implementation and complete vulnerability scanning coverage of all required databases.

Response The Census Bureau has previously addressed, and concurs with, this recommendation.

The issues identified in this recommendation were part of pre-existing plans that were communicated to the OIG and were completed prior to the soft launch for Census Bureau systems supporting the Decennial. As of March 9, 2020:

- File level encryption was active for all required resources,
- The technical DLP solution was fully functioning, and

- Vulnerability scans were running on all required databases.

The Bureau continued to strengthen both security tools and its posture throughout decennial self-response and follow up operations following our plan, as communicated before and during the time of artifact collection.

Recommendation 4. Regularly perform a thorough review of Active Directory configurations and ensure that all active accounts have the minimum access rights to fulfill operational requirements. Consider the feasibility of using specialized software tools to augment the Bureau’s review of Active Directory configurations.

Response The Census Bureau concurs with this recommendation and has addressed this issue.

The Census Bureau immediately corrected the technical issues identified during the audit and implemented a process to conduct regular checks of Active Directory using Bloodhound and other tools. The Bureau is committed to continuously improving its processes and procedures and has established comprehensive monitoring of all admin and privileged accounts.

Recommendation 5. Prioritize the enforcement of PIV and other forms of MFA by (a) establishing a procedure(s) to validate the enforcement of federal PIV requirements for all users accessing Bureau resources via government-owned computers and (b) regularly verifying that all privileged access to the Bureau network or its resources for contractors working on-site at the Bowie Computer Center or Bureau headquarters in Suitland, Maryland, is protected with MFA in accordance with federal and Department requirements.

Response The Census Bureau concurs with this recommendation and has addressed this issue.

The Census Bureau reauthorized the “Acceptable User Policy for U.S. Census Bureau Information Technology Resources,” in September 2020:

“No one may access the Census Bureau enterprise or guest networks without authorization. Office-based personnel—including headquarters, the National Processing Center and all current and future remote sites (including regional offices, contact centers, and decennial field offices)—are mandated to use their enabled PIV (personal identity verification) card for access to the network in Census Bureau facilities in accordance with HSPD-12. Personnel not working in a Census Bureau facility—field representatives, enumerators, teleworkers, and remote access—are required to use their username with

password and RSA SecurID token for primary access to the network. Procedures are in place for individuals with lost or stolen PIV cards.”

The Bureau also made substantial progress in the use of PIV authentication across all user laptops and devices and will continue work to enforce the policy as stated above.

Secondly, the Bureau is committed to ensuring continued security by regularly verifying that all privileged access to the Bureau network or its resources for contractors working on-site at the Bowie Computer Center or Bureau headquarters in Suitland, Maryland, is protected with MFA in accordance with federal and Department requirements.

If you have any questions regarding this matter, please contact Kevin Smith, CIO, at 301-763-2117.

cc: André Mendes, Chief Information Officer, Department of Commerce
Kevin Smith, Chief Information Officer, Census Bureau
Beau Houser, Chief Information Security Officer, Census Bureau
Colleen Holzbach, Program Manager for Oversight Engagement, Census Bureau
Tameika Turner, IT Security Audit Liaison, Census Bureau