

The U.S. Census Bureau's Mishandling of a January 2020 Cybersecurity Incident Demonstrated Opportunities for Improvement

FINAL REPORT NO. OIG-21-034-A

AUGUST 16, 2021

FOR OFFICIAL USE ONLY

*Final Report Contains Information Marked
FOR OFFICIAL USE ONLY*



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



August 16, 2021

MEMORANDUM FOR: Dr. Ron Jarmin
Acting Director
U.S. Census Bureau

Don Graves
Deputy Secretary of Commerce

A handwritten signature in black ink, appearing to read "Frederick J. Meny, Jr.".

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

SUBJECT: *The U.S. Census Bureau's Mishandling of a January 2020 Cybersecurity Incident Demonstrated Opportunities for Improvement*
Final Report No. OIG-21-034-A

Attached for your review is our final report on the audit of the U.S. Census Bureau's (the Bureau's) incident response process. Our audit objective was to assess the adequacy of the Bureau's process to respond to cybersecurity incidents according to federal and Departmental requirements.

We found the following:

- I. The Bureau missed opportunities to mitigate a critical vulnerability, which resulted in the exploitation of vital servers.
- II. The Bureau did not discover and report the incident in a timely manner.
- III. The Bureau did not maintain sufficient system logs, which hindered incident investigation.
- IV. The Bureau did not conduct a lessons-learned session.
- V. The Bureau continued operating servers that were no longer supported by the vendor.

Please note that portions of the introduction and findings II, III, and V of this final report have been labeled as For Official Use Only.

On July 12, 2021, and July 19, 2021, we received the Bureau's and Department's responses, respectively, to the draft report's findings and recommendations. In response to our draft report, the Bureau and Department concurred with all nine recommendations and described both completed and planned actions to address each recommendation. We summarized the Bureau's and Department's responses and provided our comments within the Summary of Agency Response and OIG Comments section of the final report. We have included the Bureau's and Department's responses in appendix B of this report.

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 the 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
Luis Cano, Chief Information Officer, Census Bureau
Colleen Holzbach, Program Manager for Oversight Engagement, Census Bureau
Corey J. Kane, Audit Liaison, Census Bureau
Tameika Turner, Audit Liaison, Census Bureau
Kemi A. Williams, Program Analyst for Oversight Engagement, Census Bureau
Ken White, Audit Liaison, OUS/EA
Joselyn Bingham, Audit Liaison, Office of the Chief Information Officer
MaryAnn Mausser, Audit Liaison, Office of the Secretary



Report in Brief

August 16, 2021

Background

Beginning on January 11, 2020, servers operated by the U.S. Census Bureau (the Bureau) were attacked using a publicly available exploit. The purpose of these servers was to provide the Bureau with remote-access capabilities for its enterprise staff to access the production, development, and lab networks. According to system personnel, these servers did not provide access to 2020 decennial census networks. The exploit was partially successful, in that the attacker modified user account data on the systems to prepare for remote code execution. However, the attacker's attempts to maintain access to the system by creating a backdoor into the affected servers were unsuccessful.

The Enterprise Security Operations Center (ESOC) is the U.S. Department of Commerce's (the Department's) primary point of contact for reporting computer security incidents within the Department and to external stakeholders. During this incident, ESOC was responsible for facilitating information sharing between the Bureau and the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Additionally, the Bureau's Computer Incident Response Team was responsible for responding to the incident.

Why We Did This Review

The objective of this audit was to assess the adequacy of the Bureau's process to respond to cybersecurity incidents according to federal and Departmental requirements.

U.S. CENSUS BUREAU

The U.S. Census Bureau's Mishandling of a January 2020 Cybersecurity Incident Demonstrated Opportunities for Improvement

OIG-21-034-A

WHAT WE FOUND

We found that the Bureau should make improvements to its cyber incident response process. Specifically, the Bureau missed opportunities to mitigate a critical vulnerability, which resulted in the exploitation of vital servers. Once the servers had been exploited, the Bureau did not discover and report the incident in a timely manner. Additionally, the Bureau did not maintain sufficient system logs, which hindered the incident investigation. Following the incident, the Bureau did not conduct a lessons-learned session to identify improvement opportunities. We also found that the Bureau was operating servers that were no longer supported by the vendor.

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. Implement procedures to promptly notify relevant system personnel when critical vulnerabilities are publicly released.
2. Frequently review and update vulnerability scanning lists to ensure all network-addressable information technology (IT) assets are identified for vulnerability scanning, and document all exceptions as part of this process.
3. Ensure all network-addressable IT assets are scanned using credentials when feasible according to Bureau-determined frequencies, but no less than DHS's *Continuous Diagnostics and Mitigation Program* guidance.
4. Review the automated alert capabilities of the Bureau's security information and event management tool to ensure a similar attack can be identified in the future.
5. Ensure Bureau incident responders comply with Departmental and Bureau requirements to report confirmed computer security incidents to ESOC within 1 hour.

We recommend that the Deputy Secretary of the Department of Commerce ensure that the Department's Chief Information Officer does the following:

6. Develop ESOC procedures for the handling of alerts from outside entities (e.g., DHS CISA) to ensure information is conveyed to Department operating units in a timely manner.

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

7. Incorporate periodic reviews of the Bureau's system log aggregation configurations to ensure all network-addressable IT assets are correctly configured.
8. Update Bureau incident response policies to include a specific timeframe prescribing when to conduct a review of lessons learned.
9. Establish plans with milestones to prioritize the decommissioning of end-of-life products.

Contents

Introduction	1
Objective, Findings, and Recommendations	2
I. The Bureau Missed Opportunities to Mitigate a Critical Vulnerability, Which Resulted in the Exploitation of Vital Servers.....	2
Recommendations	4
II. The Bureau Did Not Discover and Report the Incident in a Timely Manner	4
Recommendations	6
III. The Bureau Did Not Maintain Sufficient System Logs, Which Hindered Incident Investigation.....	6
Recommendation	7
IV. The Bureau Did Not Conduct a Lessons-Learned Session.....	7
Recommendation	7
V. The Bureau Continued Operating Servers That Were No Longer Supported by the Vendor.....	8
Recommendation	8
Summary of Agency Response and OIG Comments	9
Appendix A: Objective, Scope, and Methodology	10
Appendix B: Agency Responses	12
I. Bureau Response.....	12
II. Department Response	17

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

Beginning on January 11, 2020, [REDACTED] servers operated by the U.S. Census Bureau (the Bureau) were attacked using a publicly available exploit.¹ The purpose of these servers was to provide the Bureau with remote-access capabilities for its enterprise staff to access the production, development, and lab networks. According to system personnel, these servers did not provide access to 2020 decennial census networks. The exploit was partially successful, in that the attacker modified user account data on the systems to prepare for remote code execution.² However, the attacker's attempts to maintain access to the system by creating a backdoor³ into the affected servers were unsuccessful.

The Enterprise Security Operations Center (ESOC) is the U.S. Department of Commerce's (the Department's) primary point of contact for reporting computer security incidents within the Department and to external stakeholders. During this incident, ESOC was responsible for facilitating information sharing between the Bureau and the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Additionally, the Bureau's Computer Incident Response Team (Bureau CIRT) was responsible for responding to the incident.

¹ An *exploit* is computer code or a set of instructions "that takes advantage of a software vulnerability or security flaw. It is written either by security researchers as a proof-of-concept threat or by malicious actors for use in their operations. When used, exploits allow an intruder to remotely access a network and gain elevated privileges, or move deeper into the network." See Trend Micro. *Exploit (definition)* [online]. <https://trendmicro.com/vinfo/us/security/definition/exploit> (accessed April 23, 2021).

² *Remote code execution* is a type of vulnerability in which "an attacker is able to run code of their choosing with system level privileges on a server that possesses the appropriate weakness." Robert Shimonski and Sean-Philip Oriyano, *Client-Side Attacks and Defense* (Amsterdam: Syngress, 2012), chapter 8, quoted in ScienceDirect, *Remote Code Execution* [online]. <https://sciencedirect.com/topics/computer-science/remote-code-execution> (accessed April 23, 2021).

³ A *backdoor* is "[a]n undocumented way of gaining access to [a] computer system." See U.S. Department of Commerce National Institute of Standards and Technology Computer Security Resource Center. *Backdoor (definition)* [online]. <https://csrc.nist.gov/glossary/term/backdoor> (accessed April 23, 2021).

Objective, Findings, and Recommendations

The objective of this audit was to assess the adequacy of the Bureau's process to respond to cybersecurity incidents according to federal and Departmental requirements. Our audit focused on the Bureau's response to the January 2020 attack on its remote-access servers. We conducted our analysis after the incident response process had concluded. Appendix A provides a more detailed description of our audit objective, scope, and methodology.

We found that the Bureau should make improvements to its cyber incident response process. Specifically, the Bureau missed opportunities to mitigate a critical vulnerability, which resulted in the exploitation of vital servers. Once the servers had been exploited, the Bureau did not discover and report the incident in a timely manner. Additionally, the Bureau did not maintain sufficient system logs, which hindered the incident investigation. Following the incident, the Bureau did not conduct a lessons-learned session to identify improvement opportunities. We also found that the Bureau was operating servers that were no longer supported by the vendor.

Since the January 2020 incident, the Bureau has made changes to its incident response program. By addressing the findings and recommendations in this report, the Bureau can continue to improve and have a more effective response to future cybersecurity incidents.

I. The Bureau Missed Opportunities to Mitigate a Critical Vulnerability, Which Resulted in the Exploitation of Vital Servers

The Bureau missed opportunities to mitigate a critical vulnerability⁴ on its remote-access servers before all of them were exploited by an unknown attacker beginning on January 11, 2020. The first opportunity occurred between December 2019 and January 2020. On December 17, 2019—more than 3 weeks before the Bureau was attacked—the vendor of the remote-access servers publicly released information about the vulnerability along with steps to mitigate it. On December 31, 2019—11 days before the Bureau was attacked—the National Institute of Standards and Technology (NIST) assigned the vulnerability a severity rating⁵ of “critical,” which is the highest severity in the National Vulnerability Database (NVD).⁶ According to the Bureau, on January 2 and 9, 2020, a representative from the Bureau CIRT attended security coordination meetings hosted by CISA. The vulnerability was discussed at both meetings, and attendees received a link to mitigation steps.

⁴ “The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities.” Using CVSS version 3.0, any vulnerability with a score between 9.0 and 10.0 is considered critical. See DOC NIST National Vulnerability Database. *Common Vulnerability Scoring System* [online]. <https://nvd.nist.gov/vuln-metrics/cvss> (accessed April 23, 2021).

⁵ NIST states that CVSS scoring can be used as a factor in prioritization of vulnerability remediation activities.

⁶ The National Vulnerability Database “is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP).” “The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.” See DOC NIST NVD [online]. <https://nvd.nist.gov> (accessed April 23, 2021).

Despite the publicly available notices released in December and attending two meetings on the issue in January, the Bureau CIRT did not coordinate with the team responsible for implementing these mitigation steps until after the servers had been attacked. If the Bureau had implemented the steps on its remote-access servers, the initial compromise of the servers would have likely failed.

Additionally, the Bureau was not conducting vulnerability scanning⁷ of the remote-access servers. Federal standards⁸ and Departmental policy⁹ require the Bureau to perform regular vulnerability scanning. Bureau policy establishes the requirement to perform vulnerability scanning according to DHS's *Continuous Diagnostics and Mitigation Program* guidance.¹⁰ We found that the Bureau vulnerability scanning team maintained a list of devices to be scanned. However, the remote-access servers were not included on the list, and were therefore not scanned. This occurred because the system and vulnerability scanning teams had not coordinated the transfer of system credentials required for credentialed scanning.¹¹ Had the remote access servers been included in the required monthly vulnerability scanning, the Bureau could have identified the vulnerability and taken action to mitigate it before the incident.

The Bureau missed opportunities to mitigate the vulnerability before being exploited, which allowed an attacker to make unauthorized changes to the remote-access servers. The Bureau's firewalls blocked the attacker's attempts to establish a backdoor to communicate with the attacker's external command and control infrastructure.¹² However, unauthorized changes were still made to the remote-access servers, including the creation of new user accounts.

⁷ Vulnerability scanning is performed by “[a] network tool (hardware and/or software) that scans network devices to identify generally known and organization specific [Common Vulnerabilities and Exposures].” See DOC NIST Computer Security Resource Center. *Vulnerability scanner (definition)* [online]. https://csrc.nist.gov/glossary/term/vulnerability_scanner (accessed April 23, 2021).

⁸ DOC NIST, April 2013. *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53, Revision 4. Gaithersburg, MD: NIST, F-153. Available online at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf> (accessed April 30, 2021).

⁹ DOC, June 2019. *Department of Commerce Information Technology Security Baseline Policy (DOC ITSBP)*, Version 1.0. Washington, DC: DOC, B-14-2.

¹⁰ “The [Continuous Diagnostics and Mitigation] Program enables Federal Government departments and agencies to expand their continuous diagnostic capabilities by increasing their network sensor capacity, automating sensor collections, and prioritizing risk alerts.” See U.S. Department of Homeland Security. n.d. *Continuous Diagnostics and Mitigation Program*. Washington, DC: DHS. Available online at https://us-cert.cisa.gov/sites/default/files/cdm_files/CDM_ProgramOverview.pdf (accessed April 23, 2021).

¹¹ When performing a vulnerability scan, system administrators should specify system credentials (e.g., usernames and passwords) when technically feasible to ensure a more accurate and comprehensive scan. *DOC ITSBP*, B-14-3.

¹² “*Command and Control* consists of techniques that adversaries may use to communicate with systems under their control within a victim network.” See MITRE. *Command and Control* [online]. <https://attack.mitre.org/tactics/TA0011/> (accessed April 23, 2021).

Recommendations

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

1. Implement procedures to promptly notify relevant system personnel when critical vulnerabilities are publicly released.
2. Frequently review and update vulnerability scanning list(s) to ensure all network-addressable information technology (IT) assets are identified for vulnerability scanning, and document all exceptions as part of this process.
3. Ensure all network-addressable IT assets are scanned using credentials when feasible according to Bureau-determined frequencies, but no less than DHS's *Continuous Diagnostics and Mitigation Program* guidance.

II. The Bureau Did Not Discover and Report the Incident in a Timely Manner

During the attack on the remote-access servers, the Bureau's firewalls blocked¹³ the attacker's attempts to communicate from the remote-access servers to its command and control infrastructure as early as January 13, 2020. However, the Bureau was not aware that the servers had been compromised until January 28, 2020, more than 2 weeks later. We found that this delay occurred because, at the time of the incident, the Bureau was not using a security information and event management tool (SIEM)¹⁴ to proactively alert incident responders of suspicious network traffic. Instead, the Bureau's SIEM was only being used for reactive, investigative actions. By not using a SIEM to generate automated security alerts at the time of the incident, the Bureau was delayed in confirming that the remote-access servers had been exploited. During our fieldwork, the Bureau provided evidence that it has since improved its SIEM tool by using an automated alert capability.

On January 15, 2020, the Bureau received a list of malicious internet protocol (IP) addresses from an information sharing partner that were being used to conduct the exploit.¹⁵ The Bureau's Security Operations Center (SOC)¹⁶ searched its network traffic history for these IP addresses and determined that there had not been any successful connection attempts.

¹³ According to the Bureau, the attacker's attempts to communicate outside the network failed because the Bureau had segmented its network as part of standard security practices.

¹⁴ A SIEM is an "[a]pplication that provides the ability to gather security data from information system components and present that data as actionable information via a single interface." See DOC NIST Computer Security Resource Center. *Security information and event management (SIEM) tool (definition)* [online]. https://csrc.nist.gov/glossary/term/security_information_and_event_management_SIEM_tool (accessed April 27, 2021).

¹⁵ Information sharing partners are "[o]rganizations that share cyber threat information [to] improve their own security postures as well as those of other organizations." See DOC NIST, October 2016. *Guide to Cyber Threat Information Sharing*, NIST Special Publication 800-150. Gaithersburg, MD: NIST, ii. "Cyber threat information is any information that can help an organization identify, assess, monitor, and respond to cyber threats." DOC NIST, *Guide to Cyber Threat Information Sharing*, ii. Available online at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf> (accessed April 27, 2021).

¹⁶ At the time of this incident, personnel from the Bureau's SOC were responsible for augmenting Bureau CIRT staff in handling and responding to cybersecurity incidents.

We found evidence showing this conclusion was inaccurate. At the time of the Bureau's search, one of the remote-access servers was trying to communicate to a malicious IP address outside of the Bureau's network. The Bureau's SOC misidentified the direction of this malicious network traffic and concluded it had been blocked before entering the Bureau's network. Malicious traffic originating from inside a network is a strong indicator that a server is compromised. This missed opportunity to positively identify that one of its servers had been exploited may have further delayed the Bureau's response to the attack.

Moreover, we found that the Department's ESOC did not immediately share critical information with the Bureau regarding the exploited remote-access servers, which contributed to the Bureau's delay in discovering the attack. ESOC was responsible for coordinating information sharing between Department bureaus and outside entities such as CISA. On January 16, 2020, ESOC received a report from CISA indicating the Bureau's remote-access servers had been attacked and requesting verification of whether a compromise had occurred. Although ESOC began verifying the content of CISA's report, we found no indication that ESOC provided this critical information to the Bureau. On January 30, 2020, CISA reached out to ESOC again with a second request to investigate. ESOC forwarded this request to the Bureau, and the Bureau CIRT discovered on the following day that all [REDACTED] of its servers had been compromised. One of the reasons this delay occurred was because ESOC's procedures lacked criteria for how the report is processed and shared with the affected bureau.

We also observed additional delays in the Bureau's response to this incident. On January 28, 2020, prior to receiving CISA's second request for the Department to investigate, the Bureau had run an indicator of compromise (IOC)¹⁷ script on just [REDACTED] remote-access servers in the lab environment. The report produced by this script confirmed that these servers had been exploited by an attacker. After system personnel removed malicious user account data that was identified in the script report, a Bureau incident responder recommended putting the exploited servers back into use. Beginning on January 31, 2020, after receiving CISA's second request to investigate the servers, the Bureau ran the IOC script on the other [REDACTED] servers and confirmed that all had been exploited. Despite Departmental¹⁸ and Bureau requirements¹⁹ to report security incidents within an hour, the Bureau did not report exploitation of the servers to ESOC until February 5, 2020. These delays, caused by both the Bureau and ESOC, wasted time during the critical period following the attack, which could have compounded the damage during a more significant cyber incident.

¹⁷ The IOC script was a specialized tool used to identify signs associated with a specific exploit by generating a report that revealed whether a server had been exploited by an attacker.

¹⁸ *DOC ITSBP* states "Bureau SOC/CIRT must report confirmed computer security incidents . . . to the ESOC . . . within one hour." *DOC ITSBP*, C-12-8.

¹⁹ The Bureau's cyber incident response policy states that "ESOC will be notified of all security incidents, where the confidentiality, integrity, or availability of a federal information system is potentially compromised within one hour of reaching the agency's incident response team regardless of functional or information impact." See U.S. Census Bureau, September 2020. *Cyber Incident Response Policy*. Suitland, MD: Census Bureau, 10.

Recommendations

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

4. Review the automated alert capabilities of the Bureau's SIEM to ensure a similar attack can be identified in the future.
5. Ensure Bureau incident responders comply with Departmental and Bureau requirements to report confirmed computer security incidents to ESOC within 1 hour.

We recommend that the Deputy Secretary of the Department of Commerce ensure that the Department's Chief Information Officer does the following:

6. Develop ESOC procedures for the handling of alerts from outside entities (e.g., DHS CISA) to ensure information is conveyed to Department operating units in a timely manner.

III. The Bureau Did Not Maintain Sufficient System Logs, Which Hindered Incident Investigation

System logs are a crucial forensic resource that can be used to determine when an attack took place and what actions were performed. During the incident in January 2020, none of the [REDACTED] remote-access servers were sending system logs to the Bureau's SIEM. Instead, we found that [REDACTED] of the [REDACTED] servers were configured to send system logs to a SIEM that had been decommissioned since July 2018, more than 1 year before the incident. The Bureau did not finish configuring these servers' system logs to be sent to the currently operational SIEM until November 2020. The remaining [REDACTED] servers in a lab environment were configured to store their logs only on the servers themselves, because there was no SIEM available in the Bureau's lab environment. The Bureau did not begin collecting sufficient system logs for these lab servers until after our fieldwork requests in January 2021.

During incident handling in January 2020, the Bureau discovered it did not have the system logs available in its operational SIEM. The only system logs available to the Bureau were saved locally on the remote-access servers. The Bureau attempted to investigate using these local logs. However, all remote-access servers were configured to use the vendor's default log size. By the time the Bureau was reviewing forensic evidence, the system logs no longer contained a full record of the attack. As a result of the logging misconfigurations and the vendor's default log size setting, the Bureau did not have sufficient system logs available for analysis after the incident, which hindered incident investigation. Without improving its logging capabilities, the Bureau cannot thoroughly track actions taken by attackers, and therefore may not be well prepared to respond to future, more impactful incidents.

Recommendation

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

7. Incorporate periodic reviews of the Bureau's system log aggregation configurations to ensure all network-addressable IT assets are correctly configured.

IV. The Bureau Did Not Conduct a Lessons-Learned Session

Holding a lessons-learned session among incident responders and other stakeholders shortly after an incident can help the organization improve its processes and learn from any mistakes. We found that the Bureau did not hold a formal lessons-learned meeting, round-table, or collaborative session for this incident at any level within the organization. Both Departmental²⁰ and Bureau policies²¹ encourage holding a lessons-learned session after an incident.

One incident responder stated that the team was consumed with responding to data requests from outside entities, which interfered with holding a lessons-learned session. Furthermore, after reviewing Bureau incident response policies and procedures, we were unable to locate any requirement or guideline prescribing the timeframe in which to hold a lessons-learned session. NIST recommends holding a lessons-learned meeting within several days after the end of an incident.²²

By not holding a lessons-learned session, the Bureau was not able to fully improve its processes based on the experience gained and insufficiencies recognized following the incident. As reflected in our other findings, the Bureau had opportunities to improve its incident response process. A lessons-learned session could have allowed the Bureau to identify improvement opportunities for both its procedural and technical security measures.

Recommendation

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

8. Update Bureau incident response policies to include a specific timeframe prescribing when to conduct a review of lessons learned.

²⁰ DOC ITSBP, B-8-2.

²¹ U.S. Census Bureau, September 2019. *Cyber Incident Response Policy*. Suitland, MD: Census Bureau, 7.

²² DOC NIST, August 2012. *Computer Security Incident Handling Guide*, NIST Special Publication 800-61, Revision 2. Gaithersburg, MD: NIST; 38. Available online at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> (accessed April 23, 2021).

V. The Bureau Continued Operating Servers That Were No Longer Supported by the Vendor

While the Bureau migrated the capabilities of [REDACTED] of the [REDACTED] remote-access servers to new server hardware in September and December 2020, we found in February 2021 that the Bureau was still running all of the original servers that were involved in the incident. All [REDACTED] of these servers were operating past their end-of-life date, which occurred on January 1, 2021. The end-of-life date signified that the vendor would no longer provide security patches or maintenance for the product. Under these conditions, the Bureau would be vulnerable to any newly discovered exploits.

The Bureau did not prioritize the decommissioning of these aging remote-access servers. We found [REDACTED] servers were still publicly accessible and had continued to be used for remote access to a lab environment. The Bureau stated that it originally intended to pursue alternative solutions for these lab servers, but later decided to migrate to a newer version from the same vendor. This process delayed the migration to new, supported hardware for the lab environment until after the end-of-life date. After we briefed Bureau leadership on these publicly accessible servers, the Bureau took immediate action to ensure the servers were no longer accessible via the Internet while it continued the migration process. We also found the Bureau continued operating the remaining [REDACTED] servers on its internal network. After our fieldwork requests, the Bureau promptly made plans to decommission these remote-access servers.

CISA states that “continued use of [end-of-life] software poses consequential risk to your system that can allow an attacker to exploit security vulnerabilities.”²³ Departmental policy requires the Bureau to manage end-of-life hardware, software, and funding for replacements.²⁴ The Bureau needs to improve its handling of end-of-life products to reduce the risk posed by these products.

Recommendation

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

9. Establish plans with milestones to prioritize the decommissioning of end-of-life products.

²³ DHS CISA. *Security Tip (ST04-006), Understanding Patches and Software Updates* [online]. <https://cisa.gov/tips/st04-006> (accessed March 30, 2021).

²⁴ DOC ITSBP, 20.

Summary of Agency Response and OIG Comments

On July 12, 2021, and July 19, 2021, we received the Bureau's and Department's responses, respectively, to the draft report's findings and recommendations. In response to our draft report, the Bureau and Department concurred with all nine recommendations and described both completed and planned actions to address each recommendation.

The Bureau stated in part, in response to Recommendation 5, "The cyber incident had been confirmed at the CISA and DOC ESOC level and a case number had been established prior to Census confirming the successful exploit of the vulnerability." As we verified during the audit, both CISA and ESOC relied upon the Bureau to provide confirmation of the incident. There had been no case number established by ESOC for this incident until the Bureau provided confirmation on February 5, 2020, that the servers had been exploited.

We have included the Bureau's and Department's responses as appendix B of this report.

Appendix A: Objective, Scope, and Methodology

The objective of our audit was to assess the adequacy of the Bureau's process to respond to cybersecurity incidents according to federal and Departmental requirements.

To do so, we examined the Bureau's handling of a single incident which occurred in January 2020. We evaluated the Bureau's actions during this incident according to the four stages of the NIST Incident Response Life Cycle.²⁵

- **Preparation**—establishing an incident response capability so that the organization is ready to respond to incidents, as well as preventing incidents by ensuring that systems, networks, and applications are sufficiently secure
- **Detection and Analysis**—determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem
- **Containment, Eradication, and Recovery**
 - a. *Containment*—limiting an incident before it can overwhelm resources or increase damage as well as providing time to develop a tailored remediation strategy
 - b. *Eradication*—eliminating components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited
 - c. *Recovery*—restoring systems to normal operation, confirming that the systems are functioning normally, and (if applicable) remediating vulnerabilities to prevent similar incidents
- **Post-Incident Activity**—learning and improving from the incident by conducting a lessons-learned meeting, collecting relevant metrics, and retaining any necessary evidence

To understand the Bureau's actions and accomplish our objective, we performed the following actions:

- Interviewed staff and contractors from different Bureau offices.
- Interviewed Department staff and a contractor from ESOC.
- Analyzed system records and logs from the incident.
- Examined Departmental and Bureau policies and procedures related to incident response.
- Reviewed communications between both Departmental and Bureau incident responders.

²⁵ DOC NIST *Computer Security Incident Handling Guide*, 21, 26, 35, 37, 38–41.

We also 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, 44 U.S.C. §§ 3551, et seq.
- U.S. Department of Commerce, *Information Technology Security Baseline Policy*
- U.S. Census Bureau, *Incident Response Policy* (Fiscal Year 2019)
- NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST Special Publication 800-61, Revision 2, *Computer Security Incident Handling Guide*

We did not solely rely on computer-processed data to perform this audit. Although we could not independently verify the reliability of all of the information we collected, we compared the information with other supporting documents to determine consistency and reasonableness. Based on these efforts, we believe the information we obtained is sufficient for the conclusions in this report.

We conducted our review from November 2020 through March 2021 under the authority of the Inspector General Act of 1978, as amended (5 U.S.C. App.), and Department Organization Order 10-13, dated October 21, 2020. We performed our fieldwork remotely or at Department headquarters in Washington, DC.

We conducted this performance audit in accordance with generally accepted government auditing standards. These 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: Agency Responses


I. Bureau Response



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

July 12, 2021

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

FROM: Ron S. Jarmin 
Acting Director
U.S. Census Bureau

SUBJECT: Response to *OIG Report: The U.S. Census Bureau's Mishandling of a January 2020 Cybersecurity Incident Demonstrated Opportunities for Improvement*

This memorandum serves as the formal response to the draft report by the Office of Inspector General (OIG) entitled *The U.S. Census Bureau's Mishandling of a January 2020 Cybersecurity Incident Demonstrated Opportunities for Improvement*. The Census Bureau appreciates the continued work of the OIG in conducting transparent reviews and providing recommendations that have supported the Census Bureau in maintaining and continuously improving cybersecurity methodologies and procedures.

As the Census Bureau and the OIG both concluded following this incident, there were no indications of compromise on any 2020 Decennial Census systems nor any evidence of malicious behavior impacting the 2020 Decennial counts. Furthermore, no systems or data maintained and managed by the Census Bureau on behalf of the public were compromised, manipulated, or lost because of the incident highlighted in the OIG's report. This memorandum includes general feedback and additional context to communicate the good faith efforts made by Bureau personnel to address this incident in a timely manner.

The Census Bureau welcomes recommendations proposed by the OIG, which will support our staff in addressing potential deficiencies and administer improved cybersecurity practices. The Census Bureau looks forward to a continued partnership with the OIG to better safeguard Federal and Departmental resources against future cybersecurity attacks.



[census.gov](https://www.census.gov)

Responses to Specific Sections of the Draft Report

Objective, Findings and Recommendations

Throughout this incident, the Census Bureau worked closely with partners across the Federal Government, including the Department of Commerce's Enterprise Security Operations Center (ESOC) and the Cybersecurity and Infrastructure Security Agency (CISA). The Census Bureau would like to acknowledge that this was a federal-wide incident that impacted numerous Departments and agencies. The Census Bureau's response to this incident was in line with federal direction and response activities. Bureau personnel also collaborated with security experts at the Federal Bureau of Investigation, both during and after the incident, to share emerging information.

Comments for Finding I: "The Bureau Missed Opportunities to Mitigate a Critical Vulnerability, Which Resulted in the Exploitation of Vital Servers"

- A. Paragraphs 1 and 2: The Census Bureau was made aware of mitigation steps in late December via bulletins from CISA and the National Institutes for Standards and Technology (NIST) that characterized the vulnerability as critical. Mitigations at this time consisted of configuration settings to be implemented while the vendor worked to release a patch. In mid-January, the concern escalated when it was discovered that the vulnerability was being actively exploited. At this point, CISA initiated their federal-wide incident response procedures. As exploit signatures became available, Bureau staff reacted expeditiously, following federal guidance provided by CISA and acting in a timely matter to investigate indicators of compromise to identify the incident in the Census environment.

Comments on Finding II: "The Bureau Did Not Discover and Report the Incident in a Timely Manner"

- A. Paragraphs 1 and 2: The Census Bureau's firewalls deny a significant amount of traffic on a continuous basis. Inbound blocks are based on defined rulesets that align to known cyber threats, while outbound blocks are based on best practices for network architecture. Additionally, Census firewalls rules are set to "deny all" traffic unless specifically allowed. The Census SIEM ingests data from a variety of sources, including firewalls, and generates automatic alerts based on a combination of events or activities occurring on the network, not just a block occurring on the firewall. Census agrees with the OIG that proper tuning and automated alert capabilities are key to responding promptly to potential incidents. Over the past 18 months, Census has reduced our time-to-detect incidents by 94% through improved detection and alerting capabilities. The Census Bureau strives to continuously improve remediation and detection efforts.
- B. Paragraph 4: The Census Bureau makes every effort to respond in a timely manner to all potential and confirmed incidents. The OIG states that the "Bureau did not report exploitation of the servers to ESOC until February 5, 2020," while this is an accurate

statement, it leaves out critical context that all parties were actively investigating the issue. Additionally, the investigation was dependent on receiving indicators of compromise from CISA. Upon receiving the Initial Network Analysis Report (INAR) from CISA, the Bureau was able to run specially designed indicator of compromise (IOC) scripts in the lab environment which confirmed that the vulnerability had been compromised. At that time, a case number had already been assigned indicating that an incident was confirmed and underway. Bureau staff continued to investigate, including testing in additional environments based on reports from ESOC, to determine the full scope of the incident. Once investigations were complete and additional evidence available, BOC CIRT staff reached back out to the ESOC to confirm the initial compromise in the Census environment. The Census Bureau was also able to confirm that the second stage of the attack failed based on best practice network architecture designed to prevent communications from servers from reaching the internet.

Comments on Finding III: “The Bureau Did Not Maintain Sufficient System Logs, Which Hindered Incident Investigation”

The Census Bureau has no further information to provide on this section.

Comments on Finding IV: “The Bureau Did Not Conduct a Lessons-Learned Session”

The Census Bureau has no further information to provide on this section.

Comments on Finding V: “The Bureau Continued Operating Servers That Were No Longer Supported by the Vendor”

- A. Paragraph 2: The Census Bureau strives to ensure no end-of-life hardware or software is allowed to run on the network. As acknowledged by the OIG, the Bureau staff took immediate action to disable and disconnect the end-of-life remote-access servers.

The Census Bureau follows best practices for transitioning and/or decommissioning legacy systems and was continuing to actively manage risks related to device transition. As devices neared end of life in late 2020, Bureau staff were working closely with Citrix engineers to migrate capabilities to new devices. Due to circumstances outside the Bureau’s control—including a dependency on Citrix engineers (who were already at capacity supporting customers across the Federal government who had realized greater impacts from the January 2020 attack) to complete the migration, and the COVID-19 pandemic—the migration was delayed. Although the legacy servers were not vulnerable to compromise at the time of transition and decommissioning, the Census Bureau did not, and does not disregard end-of-life concerns. The Census Bureau will take the appropriate actions to ensure that the reliability and security of systems remain a priority.

OIG Recommendations/Census Bureau Responses

Recommendation 1. Implement procedures to promptly notify relevant system personnel when critical vulnerabilities are publicly released.

Response: The Census Bureau concurs with the recommendation. The Census Bureau has implemented improvements following the January 2020 cybersecurity incident to better respond to newly identified critical vulnerabilities. Notably, the Bureau has improved information sharing across the Office of the Chief Information Officer (OCIO) to inform staff members of known vulnerabilities and reduce time to respond.

Recommendation 2. Frequently review and update vulnerability scanning list(s) to ensure all network-addressable information technology (IT) assets are identified for vulnerability scanning and document all exceptions as part of this process.

Response: The Census Bureau concurs with the recommendation. The Census Bureau understands the need to ensure asset inventories match scanning to achieve full compliance with federal requirements. The bureau appreciates the OIG for presenting this recommendation and emphasizing vulnerability scanning as a top priority.

Recommendation 3. Ensure all network-addressable IT assets are scanned using credentials when feasible according to Bureau-determined frequencies, but no less than DHS's Continuous Diagnostics and Mitigation Program guidance.

Response: The Census Bureau concurs with this recommendation.

Recommendation 4. Review the automated alert capabilities of the Bureau's SIEM to ensure a similar attack can be identified in the future.

Response: The Census Bureau concurs with this recommendation. The Census Bureau has developed automated alerting capabilities, and established information sharing procedures for improved identification of malicious network activity. Improving these capabilities based on this recommendation will further enable the Bureau to improve the identification of malicious activity and ensure the effectiveness of the overall cyber program.

Recommendation 5. Ensure Bureau incident responders comply with Departmental and Bureau requirements to report confirmed computer security incidents to ESOC within 1 hour.

Response: The Census Bureau concurs with this recommendation. The cyber incident had been confirmed at the CISA and DOC ESOC level and a case number had been established prior to Census confirming the successful exploit of the vulnerability. After receiving an official notification, the Bureau promptly confirmed the indications of compromise within the Census Bureau environment. The Census Bureau appreciates the recommendation

from OIG and will continue to place high importance on enforcing federal requirements and efficiently communicating with ESOC.

Recommendation 6. Develop ESOC procedures for the handling of alerts from outside entities (e.g., DHS CISA) to ensure information is conveyed to Department operating units in a timely manner.

Bureau Response Not Required: This recommendation is directed to the Department of Commerce ESOC for response and actions.

Recommendation 7. Incorporate periodic reviews of the Bureau's system log aggregation configurations to ensure all network-addressable IT assets are correctly configured.

Response: The Census Bureau concurs with this recommendation. Following this attack, the Census Bureau conducted a full assessment of the entire network to ensure all devices were configured correctly to send audit logs to the proper location. The Census Bureau continues to review to ensure that any misconfigured systems are updated. The Census Bureau appreciates the OIG for highlighting this issue and providing recommendations that will improve the cybersecurity posture of the Census Bureau.

Recommendation 8. Update Bureau incident response policies to include a specific timeframe prescribing when to conduct a review of lessons learned.

Response: The Census Bureau concurs with this recommendation. The Census Bureau has updated incident response playbooks to standardize lessons learned review processes following a cyber incident. The Bureau would, however, like to underscore the numerous improvements made as a result of informal lessons learned following the January 2020 incident.

Recommendation 9. Establish plans with milestones to prioritize the decommissioning of end-of-life products.

Response: The Census Bureau concurs with this recommendation and reiterates our commitment to promptly decommission near-end and end-of-life devices. As noted in the report, the devices in question have been decommissioned.

If you have any questions regarding this matter, please contact Luis Cano, CIO, at 301-763-3968.

cc: André Mendes, Chief Information Officer, Department of Commerce
Luis Cano, 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

II. Department Response



UNITED STATES DEPARTMENT OF COMMERCE
Chief Information Officer
Washington, D.C. 20230

MEMORANDUM FOR: Peggy E. Gustafson
Inspector General

FROM:

André V. Mendes

ANDRE MENDES

Digitally signed by ANDRE
MENDES
Date: 2021.07.19 10:33:42 -04'00'

SUBJECT:

Response to OIG Report: *The U.S. Census Bureau's Mishandling of a January 2020 Cybersecurity Incident Demonstrated Opportunities for Improvement*

This memorandum transmits the formal response to the draft report by the Office of Inspector General (OIG) entitled, *The U.S. Census Bureau's Mishandling of a January 2020 Cybersecurity Incident Demonstrated Opportunities for Improvement*. The Department of Commerce (DOC) Office of the Chief Information Officer (OCIO) appreciates the opportunity to review the draft report and its recommendations. Many of the lessons learned from the OIG investigation have been vital in our efforts to continuously improve the Department's incident response processes.

The DOC OCIO will provide appropriate oversight for all the corrective actions through completion.

Should you have any questions, please contact Ryan A. Higgins, at (202) 868-2322.

cc:

Luis Cano
Beau Houser
Colleen Holzbach
Tameika Turner
William Bradd
Phillip Lamb

Department of Commerce
Comments to the OIG Draft Report Entitled

*The U.S. Census Bureau's Mishandling of a January 2020 Cybersecurity Incident
Demonstrated Opportunities for Improvement*

The Department of Commerce appreciates the opportunity to review the OIG draft report on the Census Bureau's response to a January 2020 cybersecurity incident. Below is the response to the recommendation made to the Deputy Secretary of the Department of Commerce and the Department's Chief Information Officer.

OIG Recommendation #6: OIG recommends that the Deputy Secretary of the Department of Commerce ensure that the Department's Chief Information Officer does the following:

Develop Enterprise Security Operations Center (ESOC) procedures for the handling of alerts from outside entities (e.g., DHS CISA) to ensure information is conveyed to Department operating units in a timely manner.

Response: The Department concurs with this recommendation. The ESOC works closely with each Bureau to review and update standard operating procedures regularly. To support Security Operations Center (SOC) maturation as required by OMB M-19-02: *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*, Section IV: *Implementing the Federal Cybersecurity Risk Determination Report and Action Plan*, the Department undertook efforts to improve threat information sharing. This began with the development of a Cyber Threat Intelligence (CTI) collection program to increase the collection, processing, and analysis of intelligence information from a range of sources to increase cybersecurity threat awareness among the Department's Bureaus. The ESOC will update procedures for the handling of alerts from outside entities to ensure information is conveyed to Department operating units in a timely manner. Planned Completion Date: 11/30/2021

02CENS020391