

Simulated Internal Cyber Attack Gained Control of Critical Census Bureau Systems

REDACTED FINAL REPORT NO. OIG-23-004-I

NOVEMBER 22, 2022

CONTROLLED UNCLASSIFIED INFORMATION

Final Report Contains Information Marked
CONTROLLED UNCLASSIFIED
INFORMATION



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



CUI

November 22, 2022

MEMORANDUM FOR: Robert Santos
Director
U.S. Census Bureau

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

SUBJECT: *Simulated Internal Cyber Attack Gained Control of Critical Census
Bureau Systems*
Final Report No. OIG-23-004-I

Attached is the final report on our evaluation of the U.S. Census Bureau's (the Bureau's) cybersecurity posture. Our objective was to determine the effectiveness of the Bureau's cybersecurity posture against a simulated real-world attack. To do this, we conducted a covert cyber red team with six goals tailored to relevant risks.

We found that the red team was able to gain unauthorized and undetected access to a Bureau domain administrator account as well as personally identifiable information of Bureau employees; reduce the Bureau's defensive options by **CUI**  ; use insecure programs on **CUI**  to send fake emails; and carry out several malicious actions that identified 11 security weaknesses.

On October 19, 2022, the Office of Inspector General (OIG) received the Bureau's public response to the draft report's findings and recommendations, which is included within the report as appendix D. The Bureau concurred with all of our findings and recommendations.

Pursuant to Department Administrative Order 213-5, please submit to us an action plan that addresses the recommendations in this report within 60 calendar days. 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). At the request of the Bureau, redactions have been placed in the public versions of the final report and this memorandum to cover sensitive information about information technology vulnerabilities that has been labeled as Controlled Unclassified Information.

We appreciate the cooperation and courtesies extended to us by your staff during our evaluation. If you have any questions or concerns about this report, please contact me at (202) 793-2938 or Chuck Mitchell, Director for Cybersecurity, at (202) 809-9528.

Attachment

~~CUI~~

cc: Louis Cano, Chief Information Officer, Census Bureau
Beau Houser, Chief Information Security Officer, Census Bureau
Victor Troyan, Assistant Division Chief Cybersecurity Operations, Census Bureau
Corey J. Kane, Audit Liaison, Census Bureau
Colleen Holzbach, Program Manager for Oversight Engagement, Census Bureau
Kemi Ariana Williams, Program Analyst for Oversight Engagement, Census Bureau
Ken White, Audit Liaison, OUS/EA
Maria Hishikawa, IT Audit Liaison, OCIO
MaryAnn Mausser, Audit Liaison, Office of the Secretary



Report in Brief

November 22, 2022

Background

One of the U.S. Census Bureau's (the Bureau's) well-known functions is the decennial census which, among other things, dictates the apportionment of congressional lawmakers in the U.S. House of Representatives. These data are also used to define congressional districts and distribute billions of dollars in federal funds for infrastructure and public services, such as highways, hospitals, and schools. More broadly, the Bureau collects, analyzes, and publishes demographic and economic statistics which can include sensitive financial and personal information on U.S. residents and businesses.

The Bureau uses an information technology enterprise network to store, process, and transmit data.

In January 2020, hackers were able to successfully exploit a security weakness in the Bureau's virtual desktop infrastructure just prior to the official start of the 2020 Census. The hackers' success came from exploiting a known vulnerability, and our office reported on this incident in an August 2021 report. In light of that incident, we launched a cyber red team to provide a realistic assessment of the Bureau's susceptibility to advanced cyber threats. A cyber "red team" is the deliberate use of an emulated threat against organizational assets to test the defenses of an organization.

Why We Did This Review

Our audit objective was to determine the effectiveness of the Bureau's cybersecurity posture against a simulated real-world attack.

U.S. Census Bureau

Simulated Internal Cyber Attack Gained Control of Critical Census Bureau Systems

OIG-23-004-I

WHAT WE FOUND

We determined that the Bureau did not have an effective cybersecurity posture in place to protect against a simulated real-world attack. Specifically, we found that the red team:

- I. Gained unauthorized and undetected access to a Bureau domain administrator account.
- II. Gained unauthorized and undetected access to personally identifiable information (PII) of Bureau employees.
- III. Reduced the Bureau's defensive options by CUI
- IV. Used insecure programs on [REDACTED] to send fake emails.
- V. Carried out several malicious actions that identified 11 security weaknesses.

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 a process to periodically review and verify that Active Directory permissions are protected from common attacks, are aligned to least privilege principles, and that configurations adhere to least functionality principles.
2. Implement advanced authentication security controls and verify proper protection against the discovered vulnerabilities.
3. Develop alerts that align with common detection methods for known attacks and periodically verify that these detection methods remain current and effective.
4. Verify that file shares containing PII have (a) proper permissions that follow least privilege principles and (b) permissions are periodically reviewed.
5. Implement a control for sensitive data CUI
6. Update logging configuration requirements to collect information necessary for reporting breaches related to sensitive PII.
7. CUI
8. Establish a process to periodically test and inspect Bureau websites and web applications for vulnerabilities and susceptibility of malicious input.
9. Formalize and continue to perform a process of cleaning and removing legacy code in Bureau systems.
10. Conduct a full after-action review on the detailed red team report and develop a corrective action plan to resolve specific issues identified by the red team, as appropriate, and based on risk.

CUI

Contents

Introduction.....	1
Objective, Findings, and Recommendations	3
I. The Red Team Gained Unauthorized and Undetected Access to a Bureau Domain Administrator Account.....	4
Recommendations	6
II. The Red Team Gained Unauthorized and Undetected Access to PII of Bureau Employees	7
Recommendations	8
III. The Red Team Reduced the Bureau’s Defensive Options by CUI	8
Recommendation	9
IV. The Red Team Used Insecure Programs on CUI to Send Fake Emails.....	9
Recommendations	11
V. The Red Team Carried Out Several Malicious Actions That Identified 11 Security Weaknesses.....	11
Recommendation	12
Appendix A: Objective, Scope, and Methodology	14
Appendix B: Detailed Red Team Engagement.....	19
Appendix C: Technology Descriptions and Definitions.....	25
Appendix D: Agency Response.....	27

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

Introduction

In January 2020, hackers were able to successfully exploit a security weakness in the U.S. Census Bureau's (the Bureau's) virtual desktop infrastructure¹ just prior to the official start of the 2020 Census. The hackers' success came from exploiting a known vulnerability, and our office reported on this incident in an August 2021 report.² In light of that incident, we launched a cyber red team to provide a realistic assessment of the Bureau's susceptibility to advanced cyber threats.

A cyber "red team" is the deliberate use of an emulated threat against organizational assets to test the defenses of an organization. It is a realistic method to test a program of controls for weaknesses or vulnerabilities rather than testing single controls in isolation. Our evaluation was conducted in a covert manner (at least, to the maximum extent that was possible) to avoid any bias in testing results. The red team process emulates the stages of a real-world cyberattack, as displayed in figure 1.

Figure 1. General Cyberattack Steps



Source: OIG, based off the MITRE ATT&CK Framework. See The MITRE Corporation, *MITRE ATT&CK Framework* [online]. <https://attack.mitre.org> (accessed January 5, 2022)

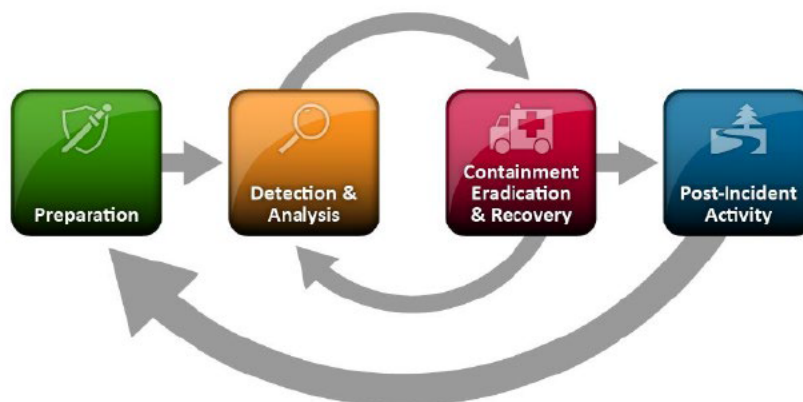
¹ Virtual desktop infrastructure is a technology that allows employees to access information technology (IT) services and data remotely. For more information on virtual desktop infrastructure, see appendix C.

² U.S. Department of Commerce Office of Inspector General, August 16, 2021. *The U.S. Census Bureau's Mishandling of a January 2020 Cybersecurity Incident Demonstrated Opportunities for Improvement*, OIG-21-034-A. Washington, DC: DOC OIG. Available online at <https://www.oig.doc.gov/OIGPublications/OIG-21-034-A.pdf> (accessed April 11, 2022).

One of the Bureau's well-known functions is the decennial census which, among other things, dictates the apportionment of congressional lawmakers in the U.S. House of Representatives. These data are also used to define congressional districts and distribute billions of dollars in federal funds for infrastructure and public services, such as highways, hospitals, and schools. More broadly, the Bureau collects, analyzes, and publishes demographic and economic statistics, which can include sensitive financial and personal information on U.S. residents and businesses. Titles 5, 13, and 26 of the United States Code (U.S.C.) require the safeguarding of this sensitive information. Thus, the Bureau has an important task: defend this data from threats, including those from well-funded criminal organizations or adversarial nation-states.

The Bureau uses an information technology enterprise network to store, process, and transmit data. Two key security functions that protect the Bureau's network are its incident response program and security operations center. A security operations center monitors information and alerts from incoming and outgoing network traffic, endpoints, and various other security tools. Incident responders then investigate alerts and take action to contain, eradicate, and recover from the incident as a part of the response lifecycle (see figure 2). For more information on related technologies that were relevant to our evaluation, see appendix C.

Figure 2. Incident Response Lifecycle



Source: Department of Commerce National Institute of Standards and Technology, August 2012. *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*, Special Publication 800-61, Rev. 2. Gaithersburg, MD: NIST, pg. 21

CUI

Objective, Findings, and Recommendations

The objective of this evaluation was to determine the effectiveness of the Bureau's cybersecurity posture against a simulated real-world attack. We contracted with a security firm to conduct a covert cyber red team with six goals tailored to relevant risks, including access to or manipulation of census data. The contractor performed attacks from outside and inside the Bureau's internal network. Once the active testing was completed, OIG performed additional analyses on the most important issues discovered by the red team. Appendix A contains additional details regarding our scope and methodology and Appendix B contains a detailed summary of the red team engagement.

While the red team identified issues with the Bureau's external defenses, key security controls **CUI** kept the red team from establishing an initial foothold on the internal network. At this point, we coordinated an assumed breach scenario.³ Once the Bureau provided the red team with an internal foothold under an assumed breach scenario, we determined that the Bureau did not have an effective cybersecurity posture in place to protect against a simulated real-world attack.

Specifically, we found that the red team was able to gain unauthorized and undetected access to a Bureau domain administrator account as well as personally identifiable information (PII) of Bureau employees; reduce the Bureau's defensive options by **CUI** **CUI** use insecure programs on **CUI** to send fake emails; and carry out several malicious actions resulting in IT security weaknesses.

CUI

The Bureau was responsive to the red team's findings by taking immediate action to address some issues raised during our evaluation and working toward long-term improvements. When applicable, we note these activities along with our findings throughout this report.

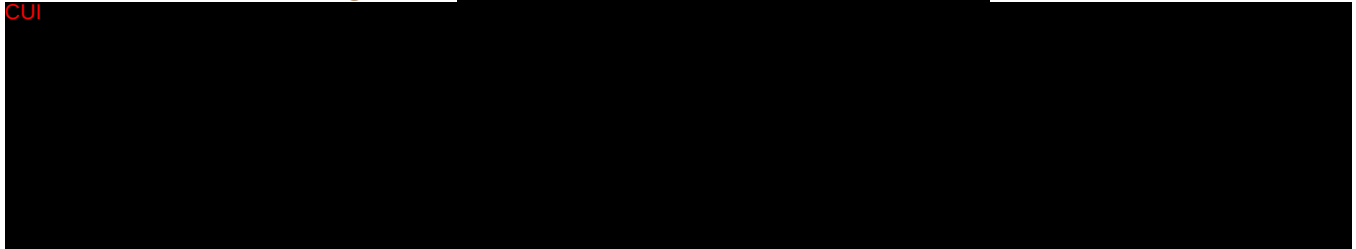
³ An *assumed breach scenario* is when the red team's access to the internal target network is facilitated, and not gained through organic red team exploitation. This method considers the perspective that an advanced and well-resourced attacker, with enough time will inevitably breach outer defenses to establish an internal foothold. It focuses on testing security countermeasures on a network after an attacker has breached network defenses.

CUI

I. Red Team Gained Unauthorized and Undetected Access to a Bureau Domain Administrator Account

Red team operators identified and leveraged a multiple-step attack path to control a domain administrator account (see figure 3). Once a domain administrator account is under their control, advanced threat actors can pivot across a network, evade security defenses, maintain a foothold on the network, access sensitive files, and run malicious commands. By bypassing multiple security countermeasures and evading detection by the Bureau's security staff, the red team demonstrated a critical threat to the Bureau's information security.

Figure 3. **CUI**



After reviewing the red team attack and performing follow-on fieldwork with the Bureau, our office identified three main categories of weaknesses: (1) account and configuration management, (2) weak passwords, and (3) insufficient incident detection and alerting.

I. Account and configuration management

The U.S. Department of Commerce's (the Department's) *Information Technology Security Baseline Policy (ITSBP)*⁴ requires least functionality and least privilege. *Least functionality* is a configuration control that requires information systems only employ the minimum functionality or capabilities necessary for proper use. *Least privilege* is an account management control that requires system users are only given the privileges or permissions that are necessary for users' work.

CUI [redacted], red team operators found **CUI** [redacted] that they used to run malicious commands **CUI** [redacted]. **CUI** [redacted]

CUI [redacted] The tool's developer had released warnings concerning the tool's lack of comprehensive logging and advanced security mechanisms and released a new version that resolved those issues. However, the older version was still available since the Bureau did not restrict access to or disable the tool. The availability of this outdated tool facilitated the domain administrator compromise and allowed the red team to run commands as a user with excessive privileges, **CUI** [redacted].

⁴ DOC, June 2019. *Department of Commerce Information Technology Security Baseline Policy (ITSBP)*, Version 1.0. Washington, DC: DOC, Annex B-5 & Annex B-1.

CUI**CUI****Figure 4.****CUI****CUI**

2. Weak passwords

Passwords are mechanisms to verify (or authenticate) that a user is who they claim to be. To do that effectively, the *ITSBP* requires that systems (1) enforce the use of complex passwords and (2) are configured to store passwords in a manner that is resistant to attacks.⁶ However, the Bureau's Active Directory was configured to allow an older password storage method with known weaknesses.

CUI

The password storage issue was resolved during the evaluation, but even passwords that meet the Bureau's current complexity standards can still be vulnerable if employees make those passwords easy to guess. To reinforce the need for stronger authentication mechanisms, the Executive Branch is moving federal agencies toward a more resilient cybersecurity model called "zero trust architecture."⁹ Zero trust architecture encourages advanced authentication controls beyond passwords to defend against the type of threats that were emulated in this

CUI

⁶ *ITSBP*, Annex B-7.

CUI

⁹ Office of Management and Budget, January 26, 2022. *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, M-22-09. Washington, DC: OMB. Available online at <https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf> (accessed May 17, 2022).

CUI

evaluation. This is a longer-term requirement which the Bureau must meet by the end of fiscal year 2024.

3. *Insufficient incident detection and alerting*

With a **CUI** account under their control, the red team used **CUI** to ultimately escalate access to a domain administrator account (see figure 4). **CUI**

The *ITSBP* requires the Bureau to record and monitor the activity on its network and to respond to alerts about potential security incidents.¹⁰ However, we found that even though the malicious activity was mostly captured in logs, the domain administrator attack still went undetected by the Bureau. Although the red team was using **CUI** attack types, the Bureau had not configured its security tools to generate alerts on these specific indicators of attacks and activities. For example, within a **CUI** the red team made approximately **CUI** to the Bureau's **CUI** servers **CUI**. To put that in perspective, this was an almost **CUI** increase over the average Bureau user activity. Such a significant increase in user behavior was a missed opportunity for the Bureau to detect the red team's attack in real-time. Due to the lack of alerts, the red team assumed domain administrator privileges while remaining undetected (see figure 3, step 3).

By leveraging available software, user accounts with excessive permissions, and weak passwords, the red team was able to demonstrate a critical threat to the Bureau's information security. This combined with the Bureau's lack of alerts for known attack methods also demonstrated an opportunity for the Bureau to improve its incident response program.

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 a process to periodically review and verify that Active Directory permissions are protected from common attacks, are aligned to least privilege principles, and that configurations adhere to least functionality principles.
2. Implement advanced authentication security controls and verify proper protection against the discovered vulnerabilities.
3. Develop alerts that align with common detection methods for known attacks and periodically verify that these detection methods remain current and effective.

¹⁰ *ITSBP*, Annex B-3, Annex B-17, & Annex B-8.

CUI

II. Red Team Gained Unauthorized and Undetected Access to PII of Bureau Employees

In accordance with the Privacy Act, sensitive and personal data—such as Social Security numbers—must be protected by federal agencies from unauthorized disclosure.¹¹ Internally, the Department's *ITSBP* requirement of least privilege (as discussed in finding I) also applies to accessing sensitive data. The *ITSBP* additionally states that systems should be configured to detect attacks and monitor for indicators of potential attacks.¹² These system alerts would notify the appropriate personnel to address the potential attack through incident response procedures.

Red team operators identified an open file share that contained sensitive employee PII. Data included hiring forms with Social Security numbers, first and last names, and home addresses. The red team observed two instances where approximately 10 individuals appeared then were removed from this file share over the course of 2 weeks. The red team was then able to access and simulate transferring this information outside of the Bureau's network without generating any alerts, as shown in figure 2.

Through follow-up, we determined that this file share is used by the Bureau's human resources (HR) staff to transfer employee hiring forms to another system. Our analysis showed that the file permissions allowed non-HR users—**CUI** **CUI**—access to this data. As part of our follow-up, we requested log files that **CUI** but found that none existed. As such, we were unable to verify whether any unauthorized access occurred prior to our testing. We also requested any alerts **CUI** **CUI**

If this had been a real incident or breach, an incident response and investigation would have followed. According to the Department's *Breach Notification Plan*, the quantity of records that were accessed or stolen must be accounted for.¹³ This accounting would take place through system logs. Done properly, these logs would have an immutable record as to who accessed what records and when. Detailed logs support incident or breach investigation activities. Without that record of access, determining the extent of the breach would be difficult or impossible.

Once notified, the Bureau modified the file share's permissions to restrict access to the PII. While the Bureau responded to the issue, we observed that confidentiality requirements

¹¹ See the Privacy Act of 1974, as amended, 5 U.S.C. § 552a. The Privacy Act provides privacy protections for records containing information about individuals (i.e., citizens and legal permanent residents) that are collected and maintained by the federal government in a system of records and are retrieved by a personal identifier. The Privacy Act requires agencies to safeguard information contained in a system of records.

¹² *ITSBP*, Annex B-17 & Annex B-8.

¹³ See DOC Office of Privacy and Open Government, September 2020. *Department of Commerce PA, PII, and BII Breach Notification Plan*, Version 6.0. Washington, DC: DOC OPOG, chap. 5 & app. A. Available online at https://www.osec.doc.gov/opog/privacy/DOC_PA_PII_and_BII_Breach_Notification_Plan.pdf (accessed May 17, 2022).

CUI

were not met, alerts were not triggered, and system event logging was insufficient to support a privacy breach investigation.

While it is hard to quantify or predict the effects of reputational damage, personal data collection and data stewardship is central to the Bureau's mission. If individuals and businesses can't trust the Bureau with personal information, then it may degrade the Bureau's ability to perform its mission. Impacted employees would be put at greater risk for having their identities stolen and the Bureau could have incurred fines, credit monitoring costs, legal fees, and other incident response and investigation costs.

Recommendations

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

4. Verify that file shares containing PII have (a) proper permissions that follow least privilege principles and (b) permissions are periodically reviewed.
5. Implement a control for sensitive data **CUI**
[REDACTED]
6. Update logging configuration requirements to collect information necessary for reporting breaches related to sensitive PII.

III. Red Team Reduced the Bureau's Defensive Options by **CUI**

[REDACTED]

CUI
[REDACTED]

CUI
[REDACTED]

CUI
[REDACTED]

[REDACTED]

~~CUI~~~~CUI~~~~CUI~~~~CUI~~~~CUI~~

Recommendation

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

7.

~~CUI~~

IV. Red Team Used Insecure Programs on ~~CUI~~ to Send Fake Emails

Erroneous or intentionally malicious inputs can be used to exploit vulnerabilities in a website. To prevent such attacks, the *ITSBP* requires that user and automated information

~~CUI~~

CUI

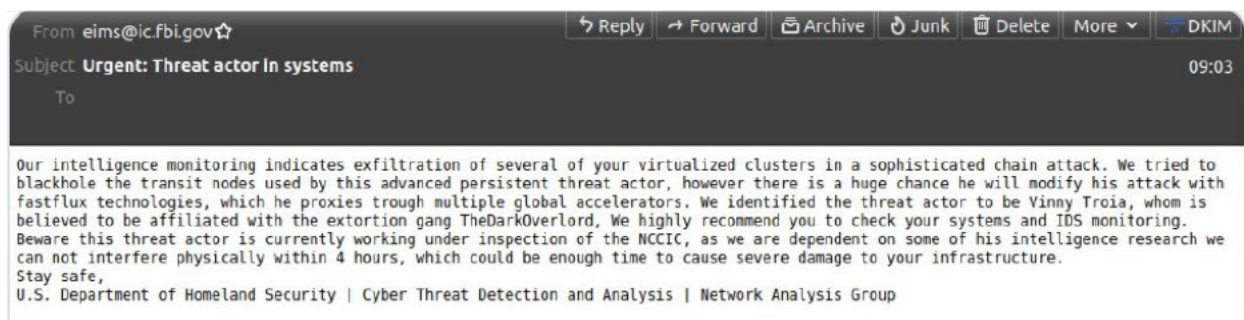
inputs are checked for accuracy, completeness, and validity.¹⁹ As discussed in finding I, the *ITSBP* also requires that systems employ least functionality.

Red team operators found **CUI** with a program that allowed **CUI** the ability to send emails from an @census.gov address. **CUI** emails could be sent to the Bureau's users or to external email addresses. The red team exploited this to send phishing emails **CUI** Bureau email addresses. The campaign received **CUI** before the emails were blocked and purged by security staff.

The Bureau's security operations were alerted to the phishing attempt just minutes after the first email reached users' inboxes. Minutes thereafter, security personnel initiated a coordinated call with various security stakeholders to address the incident. **CUI** **CUI**, the Bureau identified and disabled the insecure program. They also determined that this program was old and no longer needed for that office's operations. As an additional follow-up action to prevent any similar issues, the Bureau's Chief Information Officer coordinated stakeholders to purge old and unneeded programs from the Bureau's applications. During our follow-up, we confirmed that the Bureau **CUI**

A similar attack impacted the U.S. Department of Justice (DOJ) and was reported nationally in November 2021.²⁰ This similar attack sent a fake cybersecurity warning to thousands of email addresses, posing as the DOJ and the U.S. Department of Homeland Security (see figure 5). Given that the Bureau's mission involves collecting personal data from U.S. residents, an attacker could have exploited the public's trust to send thousands of requests for personal or otherwise sensitive information. It could have also been used to distribute malware links containing malicious code such as ransomware, for example.

Figure 5. Email Sent from Malicious Actor Impersonating the DOJ



Source: *The Verge*

¹⁹ *ITSBP*, Annex B-17.

²⁰ See Emma Roth, "The FBI's email system was hacked to send out fake cybersecurity warnings," *The Verge*, November 14, 2021. Available at <https://www.theverge.com/2021/11/14/22781341/fbi-email-system-hacked-fake-cybersecurity-warnings> (accessed March 16, 2022).

Recommendations

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

8. Establish a process to periodically test and inspect Bureau websites and web applications for vulnerabilities and susceptibility of malicious input.
9. Formalize and continue to perform a process of cleaning and removing legacy code in Bureau systems.

V. Red Team Carried Out Several Malicious Actions That Identified II Security Weaknesses

The Federal Information Security Modernization Act of 2014 requires federal agencies to apply safeguards for the confidentiality, integrity, and availability of information.²¹ The red team operators documented II findings of varying severity, which represented the Bureau's failure to adequately apply these safeguards to varying degrees (see table I). We focused on both the critical and high issues for additional follow-up as part of this evaluation. Specifically, our follow-up work was scoped to the capture, detection, and response by the Bureau to those specific issues. Therefore, the various causes of the remaining issues were not evaluated.

Table I. Red Team Findings

Severity	Count
Critical	1
High	6
Medium	1
Low	2
Informational	1

Source: OIG summary of findings' severity

We provided a copy of the red team's report to Bureau management during this evaluation so that they could understand the security issues and take timely action where appropriate. Security vulnerabilities can be weaved into attack chains that provide hackers with information or access to perform malicious actions; left unaddressed these vulnerabilities could be means to real attacks. Therefore, it is important that the Bureau conduct a detailed after-action review and analysis of the red team's actions to better understand the full impact of the work and to identify what led to the red team's successes.

²¹ *Federal Information Security Modernization Act of 2014*, 44 U.S.C. § 3554.

Recommendation

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

10. Conduct a full after-action review on the detailed red team report and develop a corrective action plan to resolve specific issues identified by the red team, as appropriate, and based on risk.

Summary of Agency Response and OIG Comments

In response to our draft report, the Bureau concurred with all of our recommendations. The Bureau also provided nonpublic technical comments recommending redactions and changes to the information in the report. We accepted the technical comments, as appropriate, and included them in the final version of this report. The Bureau's full public response is included within this final report as appendix D.

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

~~CUI~~

Appendix A: Objective, Scope, and Methodology

The objective of this evaluation was to determine the effectiveness of the Bureau's cybersecurity posture against a simulated real-world attack. This was accomplished through two phases. In Phase 1, our contractors ran a simulated attack to determine if and what attacks the Bureau was unable to prevent; then in Phase 2, OIG auditors evaluated if and how well issues were detected and responded to. Prior to starting any active testing or fieldwork, key preparation tasks were executed in the pre-fieldwork planning and contracting as listed below.

Pre-Fieldwork Planning and Contracting

- We awarded the red team contract to BreakPoint Labs, LLC (BPL).
- We formalized the rules of engagement and assessment plan with BPL. This plan included red team goals to guide BPL's actions and provide evidence for our office's evaluation objective.
- On ~~CUI~~, we established trusted agents in the Bureau during a discreet entrance conference to Bureau leadership and requested that they not disclose the test. (Note: We disclosed only the existence of the evaluation, the evaluation objective, the fact that we contracted specialists to perform the work, and that the evaluation would commence sometime within the next 6 months.)
- We coordinated with the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency and shared testing dates and exchanged contact information for any potential deconfliction.
- We coordinated with a Bureau liaison who was given limited information to facilitate BPL's special sworn status²² prior to conducting operations that could result in access to data.

Phase I/Sub-Objective I: Advanced Threat Prevention

Active red team testing began on ~~CUI~~. We tasked the red team with achieving six goals during phase I that aligned to paradigms for cyberattacks and to specific Bureau risks (see table A-1 and note goals 2, 3, and 4, specifically). These red team goals were also designed to generate results that our office could use to address our evaluation objective. For example, the red team's success or failure of goal 1 would provide evidence on whether an advanced attacker could or could not gain persistent internal access from outside of the network.

The testing was split into two stages: external and internal. The red team first performed testing against the Bureau's public-facing systems. The testing started without providing any

²² Special sworn status requires a background check and certification through training on how to handle sensitive Title 13, Title 26, and PII data that the Bureau processes, stores, and transmits.

CUI

information about the Bureau's security posture to the red team.²³ We refer to this as "no-knowledge" testing and used it to model the approach that an actual remote threat actor would take.²⁴

If external testing yielded a persistent foothold into the Bureau's internal network (see **sub-objective I.a**), then testing would have proceeded without interruption into the internal testing stage. However, since the red team could not achieve internal access via the no-knowledge approach, a strategy of marginal whitecards²⁵ was used. As soon as a whitecard was used, this evaluation was no longer a no-knowledge test. When it became apparent that an internal foothold would not be accomplished in a timely manner, we facilitated red team access in an assumed breach scenario.²⁶ This modeled a scenario where it is assumed that the outer defenses were breached and focuses testing on what actions a threat may or may not be able to achieve once inside the network. This is a common approach to red team testing, since highly resourced threat actors such as nation-states have demonstrated the use of sophisticated and previously unknown exploits that provide access to target networks.

Table A-1. Red Team Goals

Goal #	Description
1	Gain persistent network access (through no-knowledge external testing scenario)
2	Access sensitive data (particularly Title 13 and/or Title 26 data)
3	Demonstrate ability for write access to sensitive data
4	Demonstrate ability for bulk data exfiltration
5	Perform red team actions covertly (i.e., without detection)
6	Achieve domain administrative privileges

Source: OIG summary of red team goals

Phase I sub-objectives and relevant fieldwork included the following:

- **Sub-objective I.a.** To determine if a red team could penetrate the Bureau network via no-knowledge testing, between **CUI** the red team conducted the following activities:
 - From **CUI** passive reconnaissance and Open-Source Intelligence was performed on the Bureau's public-facing systems. (**Note:** Reconnaissance was an ongoing process even as the red team performed attacks.)
 - Following passive reconnaissance, from **CUI** the red team performed no-knowledge active attempts to access the Bureau's systems

²³ Our office did provide a confirmation of the Bureau's public-facing Internet Protocol (IP) addresses to the red team prior to active testing. This was necessary to ensure that the red team was only testing Bureau systems.

²⁴ No-knowledge testing is also known as "black box testing."

²⁵ A whitecard is a term of art for any information, access, or assistance provided to the red team during the engagement to artificially provide progress towards their goals.

CUI

via phishing and the exploitation of vulnerabilities. Successful malicious actions were recorded.

- Whitecards were provided, as shown in table A-2.
- **Sub-objective 1.b.** To determine if and what malicious actions could be performed by the red team, we recorded the specific malicious actions that the red team successfully achieved against the Bureau's network during internal and external testing. Successful malicious actions are evidence of threats that the Bureau was unable to prevent. Testing was concluded after the red team achieved domain administrator credentials.²⁷

Internal testing took place from **CUI**

- Following the conclusion of active testing, our office facilitated a technical out-briefing between the Bureau and the red team. This allowed a general sharing of lessons learned and an explanation of strengths and weaknesses observed during the testing.

The red team was granted clearance to target any Bureau system or user to achieve its six goals (see table A-1). While this is a comprehensive scope of *potential* targets, the red team opportunistically focused on a smaller scope of systems as opportunities to further its goals were presented. Therefore, this evaluation cannot infer the cybersecurity posture of every system that is owned and operated by the Bureau. Other system vulnerabilities or issues may have existed across the Bureau's enterprise infrastructure during our testing period that were not uncovered in this evaluation.

The rules of engagement prohibited the use of (a) a denial of service or (b) distributed denial of service attacks. This ensured that the evaluation would not negatively impact the Bureau's activities. We cannot draw any conclusions as to the Bureau's susceptibility to denial of service or distributed denial of service attacks.

Social engineering activities were in scope, thus allowing the red team to conduct phishing attacks and to virtually interact or speak with the Bureau's employees. No physical penetration testing was performed. Therefore, we cannot evaluate the effectiveness of the Bureau's physical security controls.

Table A-2. Whitecarding Summary

#	Date	Description
1	CUI	CUI Did not result in access.
2	CUI	CUI Did not result in access.

²⁷ While continued testing after the domain administrator takeover could have provided additional significant evidence for other critical malicious actions on the Bureau's network, we felt that the success of domain administrator credentials provided sufficient evidence that those actions could have been accomplished.

~~CUI~~

#	Date	Description
3	CUI CUI CUI	CUI Provided red team with unfettered access to the CUI network.

Source: OIG summary of Whitecarding activities

Phase 2/Sub-Objective 2: Advanced Threat Detection and Response

While phase 1 was performed primarily by BPL under the supervision of our office, phase 2 was primarily performed by our office via interviews with Bureau personnel and analysis of provided evidence.

Phase 2 sub-objectives and relevant fieldwork included the following:

- We analyzed the red team report to determine the significant issues for further review and analysis.
- Using our professional judgment, we determined our follow-up in phase 2 would focus on the critical and high findings that have the largest potential impact on the Bureau's incident response program and sensitive data loss.
 - These critical and high findings pertained to the domain administrator account takeover (finding I) and the sensitive data exposure (finding II).
 - We performed our sub-objective 2a and 2b procedures for those selected malicious actions.

For evidence of system logs and alerts, we (1) requested and analyzed data and (2) interviewed Bureau security and administrative personnel. We compared the Bureau's incident response to our red team exercise against the Bureau's documented incident response process.

- **Sub-objective 2.a.** To determine the Bureau's success in capturing malicious activity, we requested related logs. We reviewed the logs to verify whether they pertained to the malicious event and determined if the content was sufficient.
- **Sub-objective 2.b.** To determine the Bureau's success in identifying (i.e., detecting or alerting) malicious activity, we requested any alerts that were generated by systems, security tools, or users. We then reviewed those alerts.
- **Sub-objective 2.c.** To determine the Bureau's success in appropriately responding to incidents, we requested related incident tickets generated by the Bureau. We then reviewed the actions taken by the Bureau when it responded to the selected malicious actions.

Phase 2 fieldwork ended on March 17, 2022.

Interviews were held with Bureau incident response and security personnel, and in some cases, computer-generated information like logs and system alerts were reviewed and verified based on the comparison to red team actions. We determined that the data were sufficiently reliable

for the purposes of this report. Our review of internal security controls fell into the “Control Activities, Information and Communication, and Monitoring” components defined in the U.S. Government Accountability Office’s *Standards for Internal Control in the Federal Government*.²⁸ Given the wide scope of red team activities, the following various security controls—as defined in the *ITSBP* and NIST Special Publication 800-53²⁹—were relevant to our objective:

- Bureau of Census (BOC) Computer Incident Response Team (CIRT) Plan
- *Department of Commerce PA, PII, and BII Breach Notification Plan*
- AC-2: Account Management
- AU-3: Audit Events
- AC-6: Least Privilege
- AU-3: Content of Audit Records
- AU-6: Audit Review, Analysis, and Reporting
- AT-2: Security Awareness and Training
- CA-7: Continuous Monitoring
- CM-6: Configuration Settings
- CM-7: Least Functionality
- IA-5(1): Authenticator Management | Password-Based Authentication
- RA-5: Vulnerability Scanning
- SI-3: Malicious Code Protection
- SI-4: Information System Monitoring
- SI-4(4): Information System Monitoring | Inbound and Outbound Communications Traffic
- SI-4(5): Information System Monitoring | System-Generated Alerts
- SI-8: Spam Protection
- SI-10: Information Input Validation

We conducted our evaluation from August 2021 through March 2022 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 2020. We performed our fieldwork remotely.

We conducted this evaluation in accordance with *Quality Standards for Inspection and Evaluation* (January 2012) issued by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that the evidence supporting the evaluation’s findings, conclusions, and recommendations should be sufficient, competent, and relevant and should lead a reasonable person to sustain the findings, conclusions, and recommendations. We believe that the evidence obtained provides a reasonable basis for our findings, conclusions, and recommendations based on our evaluation objective.

²⁸ U.S. Government Accountability Office, September 10, 2014. *Standards for Internal Control in the Federal Government*, GAO-14-704G. Washington, DC: GAO, para. OV2.04, pgs. 7–8.

²⁹ DOC NIST, April 2013. *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, Rev. 4. Gaithersburg, MD: NIST.

~~CUI~~

Appendix B: Detailed Red Team Engagement

~~CUI~~~~CUI~~~~CUI~~~~CUI~~~~CUI~~~~CUI~~~~CUI~~

CUU

CUI

CUI

[illegible]

CUI

~~CUI~~

~~CUI~~ [Redacted]

~~CUI~~ [Redacted]

~~CUI~~ [Redacted]

~~CUI~~ [Redacted]

~~CUI~~ [Redacted]

~~CUI~~ [Redacted]

~~CUI~~ [Redacted]

CUI

CUI

CUI	CUI	CUI
CUI	CUI	CUI
CUI	CUI	CUI
CUI	CUI	CUI

CUI

CUI

CUI

CUI

CUI

CUI

CUI

CUI**CUI****CUI**

CUI	CUI	CUI
CUI	CUI	CUI
CUI	CUI	CUI
CUI	CUI	CUI
CUI	CUI	CUI
CUI	CUI	CUI
CUI	CUI	CUI
CUI	CUI	CUI

CUI**CUI****CUI****CUI****CUI****CUI****CUI****CUI****CUI**

CUI

CUI



Appendix C: Technology Descriptions and Definitions

This appendix includes (1) brief descriptions of additional technologies and (2) definitions of industry-specific phrases that were included in our evaluation. The terms and phrases included provide additional background and context.

Active Directory

Active Directory manages two major items on the Windows network: user access and security settings. Users are given access to systems and data based on their job needs. Access can be *specific*, like the ability to write to a single file, or access can be *broad*, like the ability to read all of the files in a folder. These abilities are known as “permissions.” General users typically have the most restricted permissions. They can use computers for business applications like email, but they are not allowed to change security configurations or download programs, for example. Some users require the ability to make changes in how the system functions. These users are normally called “administrators” and their access is referred to as “privileged.” Depending on their specific role, privileged users might be able to add, modify, or delete users, change permissions, download and run software, and perform other security-relevant operations. With added capability and responsibility comes additional risk. While it is important to protect any user account, it is especially important to protect privileged accounts so that bad actors cannot exploit those permissions to cause significant negative impacts.

Active Directories are critical components of the Bureau’s IT infrastructure. They maintain logical structures—known as “domains”—to manage all network resources. If deployed and managed properly, each Active Directory can provide a secure means to manage networked user accounts, workstations, servers, printers, and system configurations within its domain, as illustrated in figure C-1. Due to the nature of their role, Active Directories hold sensitive information, making them prime targets for cyberattacks.

Figure C-1. The Active Directory Concept

Source: OIG description of active directory service

File Shares

File shares are folders and files (also known as “directories”) that are accessible over a network. Access to the files may be shared by many users belonging to a pre-determined group. These folders can hold various important and sensitive information that attackers target.

Hashing Algorithms

The password storage mechanism referenced in finding I is a hashing algorithm. A hashing algorithm (or “hash”) is a set of computer instructions that creates a unique fingerprint for an input such as a computer file. This set of instructions, or algorithm, receives an input of variable length then outputs a fixed-length (e.g., 128 bits) string of letters and numbers that is unique to only that exact input: the fingerprint. A key characteristic of a hash is that it is not reversible, meaning the input to the hashing algorithm (e.g., a password) cannot be discerned from the output, or fingerprint, of the hashing algorithm.

Virtual Desktop Infrastructure

A technology used to remotely access a virtual desktop on the internal Bureau network. The user logs in over the Internet from a different computer using special software. Once the user successfully logs in, the system provides them with internal network access as if they were at their desk.

Appendix D: Agency Response



UNITED STATES DEPARTMENT OF COMMERCE
U.S. Census Bureau
Washington, DC 20233-0001

Date: Wednesday, October 19, 2022

MEMORANDUM FOR: Frederick J. Meny, Jr.
Assistant Inspector General for Audit and Evaluation
U.S. Department of Commerce
Office of Inspector General

FROM: Robert Santos 
Director
U.S. Census Bureau

SUBJECT: Public Releasable Response to *OIG Report: Simulated Internal Cyber Attack Gained Control of Critical Census Bureau Systems*

This memo serves as the publicly releasable response to the OIG report “*Simulated Internal Cyber Attack Gained Control of Critical Census Bureau Systems*.” The United States (U.S.) Census Bureau values the important role of the Office of Inspector General (OIG) in evaluating Department of Commerce (DOC) IT systems to ensure sound management, maintenance, and security. Simulating real-world, advanced attacks is one of the most effective techniques for assessing IT system resilience and cyber readiness of the target organization. Our commitment to the success of this engagement was demonstrated by the extensive support provided by the Census cyber team to establish the necessary access to complete the assessment. The red team exercise performed by OIG allowed the U.S. Census Bureau the aptitude to improve cyber defenses based on simulated attack methods.

The Bureau accepts the recommendations and findings from the report and looks forward to documenting our progress and efforts in a forthcoming detailed Action Plan. The Bureau recognizes the important role OIG plays as a catalyst for positive change throughout the Department. We look forward to future engagements as an important and unbiased measure of our continued cyber maturity.

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
Ryan A. Higgins, Chief Information Security Officer, Department of Commerce
Maria Hishikawa, IT Audit Liaison, OCIO, Department of Commerce
Dr. Ron S. Jarmin, Deputy Director, U.S. Census Bureau
Beau Houser, Chief Information Security Officer, U.S. Census Bureau
Colleen Holzbach, Program Manager for Oversight Engagement, U.S. Census Bureau
Sarah K. Lane, IT Security Audit Liaison, U.S. Census Bureau



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

02CENS020403