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

December 1, 2020

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

FROM: Mark H. Zabarsky
Principal Assistant Inspector General for Audit and Evaluation

SUBJECT: *Management Alert: The Bureau Cannot Ensure That Access to Sensitive Background Investigation Information Is Limited to Individuals Who Have a Work-Related Need to Know*
Final Memorandum No. OIG-21-011-M

Attached is a management alert on the U.S. Census Bureau's (the Bureau's) ability to safeguard sensitive background investigation information. The overall objective of our ongoing evaluation[1] is to conduct a series of reviews to determine whether the Bureau's planning and execution of 2020 Census peak operations successfully reduce risk to decennial census data quality and costs. As part of this review, we assessed whether the Bureau limits access to its Census Hiring and Employment Check (CHEC) system and background investigation documentation to current staff with a work-related need to know in order to safeguard sensitive information.

We concluded that the Bureau does not effectively restrict and monitor CHEC system roles and privileges in order to ensure that access is based on a valid authorization and limited to only what is required to accomplish assigned duties. Additionally, some staff have access to sensitive background investigation information before completion of their own required background check.

In order to ensure the security of its sensitive background investigation information, the Bureau should implement or improve controls that

1. limit users' system privileges to only those required to complete their assigned duties;
2. ensure actions to grant, modify, or revoke system access follow established procedures; and
3. restrict users' access to sensitive information until investigation requirements have been met.

[1] U.S. Department of Commerce Office of Inspector General, June 18, 2020. *Evaluation of 2020 Census Peak Operations (#2020-375)*. Washington, DC: DOC OIG.

Consistent with the Inspector General Act of 1978, as amended (IG Act),[2] we are notifying Bureau leadership of the vulnerabilities that could lead to the unauthorized access of sensitive information.

We are not requesting a formal response to this management alert, as the key issues discussed in it were briefed to cognizant Departmental officials in advance of issuance. This management alert will be posted to our public website.

If you have any questions or concerns about this memorandum, please contact me at (202) 482-3884 or Terry Storms, Division Director, at (202) 482-0055.

Attachment

cc: Laura Furgione, Chief Administrative Officer, Census Bureau
Colleen Holzbach, Program Manager for Oversight Engagement, Census Bureau
Corey J. Kane, Audit Liaison, Census Bureau
Kemi A. Williams, Program Analyst for Oversight Engagement, Census Bureau
Ken White, Audit Liaison, OUS/EA
MaryAnn Mausser, Audit Liaison, Office of the Secretary

[2] The IG Act establishes that offices of inspectors general will "provide a means for keeping the head of the establishment and the Congress fully and currently informed about problems and deficiencies relating to the administration of such programs and operations and the necessity for and progress of corrective action[.]" 5 U.S.C. App., § 2(3).

Management Alert

The Bureau Cannot Ensure That Access to Sensitive Background Investigation Information Is Limited to Individuals Who Have a Work-Related Need to Know

December 1, 2020 **Final Memorandum No. OIG-21-011-M**

Key Issue(s)

We assessed whether the U.S. Census Bureau (the Bureau) limits access to its Census Hiring and Employment Check (CHEC) system and background investigation documentation to current staff with a valid work need in order to safeguard sensitive information. We determined that the Bureau did not properly secure personally identifiable information (PII) of applicants to prevent unauthorized access.[3] Specifically:

- CHEC help desk staff are able to access sensitive background investigation information, without a work-related need-to-know basis.
- CHEC help desk staff are able to grant, revoke, and modify user access improperly.
- Census Investigative Services (CIS) does not restrict access to sensitive information until investigation requirements have been met.

The lack of internal controls increases the risk that unauthorized users will gain access to sensitive information.

Proposed Action(s) for Change

The Bureau should implement or improve controls that (1) limit users' privileges to only those required to complete their assigned duties; (2) ensure actions to grant, modify, or revoke system access follow established procedures; and (3) restrict users' access to sensitive information until investigation requirements have been met.

Background

The Bureau's CIS Division conducts background investigations of all prospective employees and contractors to ensure their suitability for employment. To support the 2020 Census, CIS has conducted more than 900,000 investigations, which help the Bureau protect the public and safeguard all sensitive data—including data collected during the decennial census.

CIS employs approximately 300 staff at Bureau headquarters in Suitland, Maryland; six regional offices; and three National Processing Centers. CIS uses the CHEC system to collect and review sensitive applicant information required to conduct background investigations. Within the CHEC system, the Bureau has defined various user roles with specific privileges that determine what background investigation

[3] *See* U.S. Department of Commerce National Institute of Standards and Technology. *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST SP 800-53 (Rev. 4). Gaithersburg, MD: DOC NIST, AC-5 (Separation of Duties) & AC-6 (Least Privilege). Available online at https://nvd.nist.gov/800-53/Rev4/family/Access%20Control (accessed October 13, 2020).

information users can access and what functions they can perform.[4] The Bureau has a process for granting, revoking, and modifying CHEC user roles for those who require access to the system to accomplish assigned duties. The process begins with a request from a "designated approver"[5] sent through the system to the CHEC help desk.[6] If someone other than a designated approver submits a request, CHEC help desk staff are instructed to validate the request, via e-mail, with a designated approver for that role.

When conducting background investigations, CIS staff have access to a variety of sensitive information. Applicants are required to submit a number of documents—including U.S. Office of Personnel Management (OPM) forms that include PII—and also to disclose current and previous residences and associates, criminal history, and delinquent federal debt.[7] CIS also requires applicant fingerprint results from the Federal Bureau of Investigation, as well as other sensitive information, depending on the position.

To help ensure that CHEC users are limited to the roles and privileges required to complete their assigned duties, the Bureau established a process to conduct semiannual reviews to "recertify" user access. The process requires designated approvers to review current user access and identify those whose roles provide access that is no longer required or requires some modification. The Bureau established the plan in July 2018; however, recertification has only been conducted once in January 2020.

Our Observations to Date

We assessed whether the Bureau limits access to the CHEC system and background investigation documentation to current staff with a valid work-related need. We determined that because of internal control weaknesses, the Bureau does not properly safeguard the PII of applicants in order to prevent unauthorized access.

1. CHEC Help Desk Staff Are Able to Access Sensitive Background Investigation Information Without a Work-Related Need to Know

We determined that CHEC help desk staff are able to access sensitive background investigation information, without a valid work-related need to know. We noted that 13 CHEC help desk staff—in addition to their required support role—had an "investigation" role, which allows them to view

[4] Our previous work on the Bureau's CHEC and CIS functions include the following: (1) DOC Office of Inspector General, April 30, 2020. *Management Alert: The Census Bureau Has Not Adjudicated Hundreds of Individuals Identified as Highest-Risk in OPM Background Investigations*, OIG-20-023-M. Washington, DC: DOC OIG; (2) DOC OIG, December 10, 2019. *IG Letter to NC Delegation re: the Census Bureau's Background Check and Hiring Process*, OIG-20-012-M. Washington, DC: DOC OIG; (3) DOC OIG, February 27, 2018. *2020 Census: The Bureau's Background Check Office Is Not Fully Prepared for the 2020 Census*, OIG-18-015-A. Washington, DC: DOC OIG; and (4) DOC OIG, September 14, 2015. *Allegations of Time and Attendance Fraud and Other Misconduct by Employees in the Census Hiring and Employment Check Office*, Investigative Report No. 14-0790. Washington, DC: DOC OIG.

[5] *Designated approvers* are select individuals throughout various Bureau program areas, whom CHEC help desk staff recognize as the source of valid requests to grant, modify, and revoke system access. The CHEC help desk maintains a list of designated approvers that is updated regularly.

[6] The CHEC help desk staff work for the Personnel Automation Clearance Services Branch under the Applications Development and Services Division. CHEC help desk staff primarily manage the system's requirements and provide technical support. Help desk staff, however, do not require privileges to view or modify background investigation information in CHEC.

[7] (1) U.S. Office of Personnel Management Optional Form 306, *Declaration for Federal Employment*, Revised October 2011; and (2) OPM Standard Form 85, *Questionnaire for Non-Sensitive Positions*, Revised December 2013.

sensitive background information and even adjudicate investigations, even though they did not have a valid work-related need. This is occurring because, first, the Bureau has not implemented internal controls that limit CHEC help desk staff to only the roles required to accomplish their assigned duties (see key issue 2). Second, during the January 2020 recertification, designated approvers did not evaluate the help desk staff's access to investigation roles because help desk staff did not include themselves in the recertification list given to designated approvers.

2. *CHEC Help Desk Staff Are Able to Grant, Revoke, And Modify User Access Improperly*

CHEC help desk staff are able to override the designated approver process designed to ensure that roles and privileges are limited to what is required for individuals to accomplish their assigned duties. Help desk staff can execute any request to grant, modify, or revoke access even though they are not designated approvers for most CHEC roles—including those roles involved in adjudicating background investigations—because there is no control within the system to prevent them from doing so. Help desk staff can do this for any role within CHEC, but particularly concerning is the fact that they have granted to themselves investigation roles, which must be limited to CIS staff who are involved in adjudicating background investigations.

Specifically, we observed CHEC help desk staff granted or revoked access without proper approval on 59 occasions. On 13 of those occasions, help desk staff—who were not designated approvers—granted each other an investigation role, which allowed them to view sensitive background information and even adjudicate investigations, although they do not require such access to accomplish their assigned duties.[8]

During our review we noted that the CHEC system was not programmed to link the record of a request—to grant, modify, or revoke access—with the record of the action to execute the request. Consequently, there was no way for CIS to monitor instances in which help desk staff were overriding the designated approver process for ensuring that roles and privileges are limited to what is required for individuals to accomplish their assigned duties. We brought this to Bureau management's attention and CHEC was reprogrammed to prevent this from occurring.

3. *CIS Does Not Restrict Access to Sensitive Information Until Investigation Requirements Have Been Met*

Before granting a user access to a CHEC investigation role that is needed to view sensitive applicant information and adjudicate cases, CIS requires the individual to submit to their own tier-2 background investigation,[9] which is a comprehensive assessment of an applicant's character and judgment.[10] Unlike a tier-1 investigation,[11] which the Bureau requires for other CHEC system roles

[8] During the January 2020 recertification process, CIS failed to revoke the investigation role privileges from 10 help desk staff; after the recertification, 3 additional help desk staff were granted an investigation role.

[9] A *tier-2* investigation is required for positions designated by OPM as "Moderate Risk, Public Trust, No National Security Sensitivity" and includes Standard Form 85P (*Questionnaire for Public Trust Positions*). It is also referred to as a "Moderate Risk Background Investigation."

[10] Based on OPM guidance, CIS grants *interim* investigation role access once it confirms that an individual has scheduled a tier-2 investigation.

[11] A *tier-1* investigation is required for positions designated by OPM as "Low Risk/HSPD-12 Credential, Non-Sensitive" and includes Standard Form 85 (*Questionnaire for Non-Sensitive Positions*). U.S. Department of Homeland

that only allow a user to view the status of a case, a tier-2 investigation gathers information related to the user's criminal activity, drug and alcohol use, and use of information technology (IT) systems, including instances of illegal or improper access; unauthorized modification, destruction, or manipulation of IT information; and unauthorized denial of access to others.

However, CIS does not have a formal policy that prohibits an employee from performing the duties of each position, or viewing sensitive background investigation information, prior to meeting their own investigation requirements. As a result, some staff who have neither completed nor scheduled their own tier-2 investigation—and who therefore cannot be assigned an investigation role in CHEC—have been given access to sensitive background information. We found that managers in the Dallas region allowed such staff to communicate with applicants during background investigations and send and receive sensitive applicant information—which is stored in a Bureau shared drive and then added to CHEC by CIS staff who possess an investigation role—in order to complete adjudications.

On September 2, 2020, we briefed the Bureau on the results of our fieldwork. The information found in this memorandum summarizes the current results of our work.

We prepared this memorandum in alignment with OIG's quality control standards and under the authority of the Inspector General Act of 1978, as amended, and Department Organization Order 10-13, dated October 21, 2020. We conducted our fieldwork in accordance with the *Quality Standards for Inspection and Evaluation* (January 2012) issued by the Council of the Inspectors General on Integrity and Efficiency.

Our Future Work

The concerns presented in this memorandum and any action taken by the Bureau as a result of this management alert will be considered in our ongoing work to evaluate the results of 2020 Census operations.

We are not requesting a formal response to this management alert, as the key issues discussed in it were briefed to cognizant Bureau officials in advance of issuance. This management alert will be posted to our public website.

Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, requires a standardized badging process, which is designed to enhance security, reduce identity fraud, and protect the personal privacy of those issued government identification. Tier-1 is also referred to as a "National Agency Check and Inquiries (NACI) Investigation."