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

August 13, 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 Census Bureau Cannot Account for the Return of All Devices Used During 2020 Decennial Census Field Operations*
Final Memorandum No. OIG-20-040-M

Attached is a management alert on the U.S. Census Bureau's (the Bureau's) oversight of laptop computers used during the 2020 Decennial Census in-field address canvassing operation. During our evaluation, we found that the Bureau was unaware that over a dozen laptop computers—which may contain Title 13 protected data[1]—were lost, missing, or stolen. In order to preserve public trust, the Bureau must improve its oversight of equipment containing protected data to ensure devices that are used in the nonresponse follow-up operation—which includes about 585,000 smartphones and tablets—are adequately tracked and the data is safeguarded against unauthorized disclosure.

On July 21 and 22, 2020, we discussed with a Bureau program manager and several decennial census senior leaders, respectively, our results, as well as our plans to issue an alert memorandum. The information found in this alert memorandum summarizes the results of our work. These discussions with Bureau personnel provided an opportunity for them to take any corrective action(s) they deemed appropriate for the upcoming nonresponse follow-up operation.

Consistent with the Inspector General Act of 1978, as amended,[2] we are notifying Bureau leadership of the potential major risks that could affect the Bureau.

[1] Under Title 13 of the U.S. Code, the Bureau cannot release any identifiable information about individuals, households, or businesses, even to law enforcement agencies.

[2] The Inspector General Act of 1978, as amended, 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).

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.

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: Sean Kinn, Chief of Staff, Acquisition Division, Census Bureau
Shamere Mack, Branch Chief, Contracts Planning Staff, Decennial Contracts Execution Office, Census Bureau
Colleen Holzbach, Program Manager for Oversight Engagement, Census Bureau
Corey J. Kane, Audit Liaison, Census Bureau
Kemi A. Williams, Program Analyst for Oversight Engagement, Census Bureau
Ken White, Audit Liaison, OUS/EA
Deborah Stempowski, Assistant Director for Decennial Census Programs (Operations & Schedule Management), Census Bureau
Michael Thieme, Assistant Director for Decennial Census Programs (Systems & Contracts), Census Bureau

Management Alert

The Census Bureau Cannot Account for the Return of All Devices Used During 2020 Decennial Census Field Operations

August 13, 2020 **Final Memorandum No. OIG-20-040-M**

Key Issue(s)

The U.S. Census Bureau (the Bureau) was unaware of lost, missing, or stolen (LMS) laptop computers by the end of the in-field address canvassing operation due to (1) inadequate communication among Bureau employees, the contractor, and subcontractor staff and (2) noncompliance with certain contract terms and processes.

- More than a dozen laptop computers—which may contain Title 13 protected data—were not correctly identified as LMS in the contractor's asset management system. For some of these laptops, the Bureau did not know the devices were LMS.
- The in-field address canvassing operation officially ended on October 11, 2019, but the Bureau was not aware until early April 2020—after our office began its evaluation—that several laptop computers were not returned.
- Even though the laptop computers that were used for address canvassing were encrypted and enrolled in a mobile device management solution, the Bureau cannot confirm that remote wipe commands sent to these LMS laptop computers successfully removed census data from the devices.

The Bureau did not provide effective oversight of the return of laptop computers used for in-field address canvassing and cannot be certain that Title 13 protected data was removed from all LMS laptops. In addition to the laptop computers we detected during our review, which was limited in scope, there could be more devices that were used for in-field address canvassing and other decennial census field operations that were not returned and not properly identified as LMS in the asset management system. The Bureau on its own had identified 70 LMS laptops; however, it has not fully reconciled the laptop computers used in address canvassing. The Bureau must improve its oversight of equipment containing protected data to ensure devices used in the nonresponse follow-up operation—which includes about 585,000 smartphones and tablets—are adequately tracked and the data is safeguarded against unauthorized disclosure.

Background

The 2020 Decennial Census consists of design changes, such as the use of technology to reduce manual effort and improve the productivity of field operations. To that end, the Bureau awarded a contract that provides devices—such as laptop computers, smartphones, and tablets—as well as the accompanying service for provisioning, kitting, and shipping devices at the beginning of an operation and receiving and removing census data from the equipment at the end of the operation. Under the contract, the Bureau ordered more than 55,000 laptop computers for in-field address canvassing. Either when Bureau employees completed their work or at the end of the operation, laptop computers were supposed to be

shipped to the contractor's facility for sanitization and decommissioning.[3] To track devices, the Bureau authorized use of an asset management system called the Intelligent Telecommunications Management System (ITMS), which documents the asset tag, serial number, shipping, delivery, end-user name, LMS status, and other information about each device.

Within 1 hour of discovering that a device is LMS, Bureau policy requires that its employees report the incident to the Decennial Service Center (DSC).[4] A DSC call handler records information about the incident in an application called Remedy Case Management (RCM).[5] RCM auto-generates e-mail notifications to other appropriate offices, who investigate the incident as reported to the call handler. The investigating office then updates the RCM case files based on information obtained during its investigation. If a device is not recovered, a request is sent to the help desk to remotely wipe census data from the device. However, the remote wipe will only work if the laptop computer is turned on and connected to the Internet.

Our Observation(s) to Date

We found that the Bureau did not provide adequate oversight to ensure that the contractor complied with certain contract terms and processes for tracking laptop computers, which contributed to the incorrect LMS status of laptop computers in ITMS. Specifically, we determined the following:

- The Bureau did not require submission of a final inventory report,[6] which would have helped with monitoring the return of all laptop computers that were shipped for in-field address canvassing.
- Contractor staff did not identify and report to the Bureau until April 2020—3 months after decommissioning of address canvassing laptop computers concluded—that three laptop computers shipped as of October 2019 had not been delivered to the decommissioning facility.[7]
- The Bureau did not detect that the subcontractor overlooked recording the updated LMS status in ITMS. Additionally, it was not until late spring 2020 that the contractor and Bureau staff discovered that a subcontractor's process for updating ITMS did not work as intended, resulting in an inaccurate LMS status for six laptop computers, which had been stolen from the decommissioning facility in December 2019.

---

[3] *Decommissioning* means a device has been collected, securely sanitized of all Bureau data, and evidence has been provided to the Bureau, which indicates that the device was successfully sanitized.

[4] DSC supports field operations for decennial census staff, which includes intake of reported information technology incidents among other services.

[5] RCM is the application the Bureau uses to record, track, manage, and report incidents involving Bureau employees and respondents who are reporting safety issues, physical or information technology security events, or possible breaches of protected data.

[6] The Bureau's decennial device as a service (dDaaS) contract requires that the contractor submit a final inventory report within 10 days of initiating any large-scale device collection or final decommissioning. The Bureau's dDaaS program manager told our office that decommissioning of laptop computers used for address canvassing was completed in December 2019.

[7] Contractor staff is responsible for tracking laptop computers that are shipped and delivered to the decommissioning facility. Bureau procedures indicate if a package is not delivered within 48 hours of the scheduled delivery date, the contractor will contact the shipping carrier to locate the package. If the package is not located within 72 hours, the contractor will report the incident to the Bureau.

We also found the Bureau did not consistently follow up on unreturned laptop computers in a timely manner, resulting in delays in determining the LMS status of laptop computers. We determined the following:

- In some instances, because of a focus on other monitoring activities, Bureau employees within the Decennial Contracts Execution Office missed reading and acting on e-mails about LMS laptop computers. As a result, there were delays in obtaining asset tag numbers and other information about unreturned laptop computers, which the subcontractor needs to record that the device is LMS in ITMS.
- When laptop computers were not returned by employees when their employment ended, Bureau managers did not consistently follow procedures to recover laptop computers. Bureau procedures require that Area Census Office supervisors make three attempts to recover property. If the property is still not returned, a demand letter must be issued. In two of the four instances where laptop computers were not recovered from former decennial census employees, demand letters were not issued. Following our office's inquiry into these instances, the Bureau issued one of the demand letters and the former employee returned the laptop.

Other than the laptop computers we noted whose LMS status was not properly identified in ITMS, we did not search for any additional other devices whose status may be incorrect in the system. Accordingly, there could be additional devices that were not returned and not properly identified as LMS in ITMS.

We were informed by the Bureau's program management office that it recently began conducting weekly meetings between responsible Bureau offices and contractor personnel to discuss issues related to LMS devices. With the significant number of smartphones and tablets expected to be used during nonresponse follow-up—devices that could be more vulnerable to loss and theft—the Bureau must react quickly to improve its oversight of devices and mitigate its risks. If action is not taken, the Bureau jeopardizes losing the public's trust in its ability to conduct a safe and secure 2020 Decennial Census.

On July 21 and 22, 2020, we discussed with a Bureau program manager and several decennial census senior leaders, respectively, our results, as well as our plans to issue an alert memorandum. These discussions with Bureau personnel provided an opportunity for them to take any corrective action(s) they deemed appropriate for the upcoming nonresponse follow-up operation.

The advisory will be posted to our public website.