Office of Inspector General
U.S. Government Accountability Office

INFORMATION SECURITY

Controls for Removing Sensitive Data from Select Media Devices Prior to Disposal Were Effective

Serving the Congress and the Nation

November 2016

OIG-17-1

Office of Inspector General
U.S. Government Accountability Office
Report Highlights

November 2, 2016

INFORMATION SECURITY

Controls for Removing Sensitive Data from Select Media Devices Prior to Disposal Were Effective

Objective

Our audit objective was to assess GAO's compliance with its policies and procedures regarding media sanitization, and to determine whether laptops and BlackBerrys ready for disposal were appropriately sanitized.

What OIG Found

GAO employees rely heavily on information technology to support the Congress in meeting its constitutional responsibilities and to help improve the performance and ensure the accountability of the federal government for the benefit of the American people. When GAO information technology equipment is obsolete or no longer usable, it is important that the data stored on electronic media such as hard drives, disks, and embedded memory, cannot be retrieved or reconstructed after it has left GAO.

Special handling and controls are required to prevent the unauthorized access, use, or disclosure of sensitive GAO data, including personally identifiable information, to anyone without an official need-to-know. Such a breach could pose significant risks to GAO by reducing public trust, creating legal liabilities, or seriously harming individuals—leading to problems such as identity theft, blackmail, or embarrassment. An effective electronic media disposal process includes tracking and properly securing media, and applying effective media sanitization techniques where data is irreversibly removed from media or the media is permanently destroyed.

To achieve our audit objective, we identified and reviewed applicable policies, procedures, and best practices. We also interviewed staff within GAO's Information Systems and Technology Services Customer Relations and Engineering and Operations groups and Property Branch. In addition, we tested laptops and BlackBerrys ready for disposal to determine if any readable data remained on the devices.

We determined that GAO policies and procedures for removal of sensitive data from excessed information technology equipment were effectively designed and implemented. Therefore, we are not making recommendations for corrective action. We shared our findings with GAO and obtained oral comments regarding our assessment of its compliance with media sanitization standards, which we incorporated, as appropriate.

November 2, 2016

Memorandum For: Gene L. Dodaro
Comptroller General of the United States

From: Adam R. Trzeciak
Inspector General

Subject: Transmittal of Office of Inspector General (OIG) Audit Report

Attached for your information is our final report, *Information Security: Controls for Removing Sensitive Data from Select Media Devices Prior to Disposal Were Effective* (OIG-17-1). The audit objective was to assess GAO's compliance with its policies and procedures regarding media sanitization, and to determine whether laptops and BlackBerrys ready for disposal were appropriately sanitized.

We determined that GAO policies and procedures for removal of sensitive data from excessed information technology equipment were effectively designed and implemented. Therefore, we are not making recommendations for corrective action. We shared our findings with GAO and obtained oral comments regarding our assessment of its compliance with media sanitization standards, which we incorporated, as appropriate.

We are sending copies of this report to the other members of GAO's Executive Committee, GAO's Audit Advisory Committee, and other managers with information technology program responsibilities. The report is also available on the GAO website at http://www.gao.gov/about/workforce/ig.html.

If you have questions about this report, please contact me at (202) 512-5748 or trzeciaka@gao.gov.

Attachment

Table of Contents

Abbreviations

BES	BlackBerry Enterprise Server
ISTS	Information Systems and Technology Services
NIST	National Institute of Standards and Technology
PII	Personally Identifiable Information
SOP	Standard Operating Procedure

Introduction

The federal government has become increasingly dependent on information systems to carry out critical operations and to process, store, and share essential information. Data for these information systems are stored on information technology equipment containing electronic media such as hard drives, disks, and embedded memory. When equipment is obsolete or no longer usable, an organization may choose to dispose of it by charitable donation, internal or external transfer, or by recycling it in accordance with applicable laws and regulations. It is important that the organization ensure that the data stored on the media cannot be retrieved or reconstructed after it has left the control of the organization. This is especially important for GAO, given that its media equipment is used to process and store sensitive data, including personally identifiable information (PII).

An effective electronic media disposal process includes tracking and properly securing media, and applying effective media sanitization[1] techniques. The information security concern regarding media sanitization and disposal resides not in the media but in the recorded information. Special handling and controls are required to prevent the unauthorized access, use, or disclosure of sensitive data, including PII, to anyone without an official need-to-know. Such a breach could pose significant risks to the federal government by reducing public trust, creating legal liabilities, or seriously harming individuals—leading to problems such as identity theft, blackmail, or embarrassment.

Objective, Scope, and Methodology

The objective of this audit was to assess GAO's compliance with its policies and procedures regarding media sanitization, and to determine whether laptops and BlackBerrys ready for disposal were appropriately sanitized. To achieve our audit objective, we identified and reviewed applicable policies, procedures, and best practices. We also interviewed staff within Information Systems and Technology Services' (ISTS') Customer Relations and Engineering and Operations groups and GAO's Property Branch. In addition, we tested laptops and BlackBerrys ready for disposal to determine if any readable data remained on the devices. Further, we determined the status of GAO's fiscal year 2016 efforts to dispose of sanitized hard drives and BlackBerrys. Finally, we shared our findings with GAO and obtained oral comments regarding our assessment of its compliance with media sanitization standards, which we incorporated, as appropriate.

We conducted this performance audit from August 2016 through November 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[1]Media sanitization refers to a process where data is irreversibly removed from media or the media is permanently destroyed.

Background

GAO's mission is to support the Congress in meeting its constitutional responsibilities and to help improve the performance and ensure the accountability of the federal government for the benefit of the American people. To carry out this mission, GAO employees rely heavily on information technology. GAO's ISTS office provides technology support to GAO's workforce of approximately 3,000 employees, 4,000 laptop workstations, and almost 450 BlackBerrys. These laptops and BlackBerrys store data on hard drives, memory cards, and embedded memory.

Laptops

In 2015, GAO purchased 4,000 new, simpler and lighter laptops to replace laptops that were over 7 years old and outdated. As GAO began deploying the new laptops in support of its operations, it also started sanitizing the older equipment. Prior to the rollout of virtual desktop infrastructure[2] in 2015, users could save work to the internal hard drive on their assigned laptops.

BlackBerrys

BlackBerry is a line of wireless handheld devices (commonly called smartphones) and services designed and marketed by BlackBerry Limited, formerly known as Research In Motion Limited (RIM). BlackBerrys can record video, take photos, play music, and perform web-browsing, e-mail messaging, and instant messaging functions.

GAO's hardware inventory, obtained during a prior information security audit, identified 445 BlackBerrys as of December 2014.[3]

In fiscal year 2016, GAO initiated an effort to replace all BlackBerrys with Apple iPhones and retire the BlackBerry Enterprise Server (BES) that supported the BlackBerrys on September 30, 2016. Users were directed to turn in their old BlackBerrys to ISTS in exchange for a new iPhone. ISTS also provided users with instructions on saving BlackBerry data and setting up an Apple ID prior to the equipment exchange.

[2]Virtual desktop infrastructure is a method of running desktop operating systems and applications inside virtual machines that reside on servers in the GAO data center. Similarly, data is stored on the GAO network rather than the laptop's hard drive. The virtual desktop, applications, and data can then be accessed remotely by a multitude of computing platforms (GAO laptop, home computer, tablet, etc.).

[3]OIG, *Information Security: Review of GAO's Program and Practices for Fiscal Years 2014 and 2015*, OIG-16-2 (Washington, D.C.: Mar. 28, 2016).

Media Sanitization of Laptops and BlackBerrys Prior to Disposal was Effective

We determined that GAO has effective policies and procedures for removal of sensitive data from laptops and BlackBerrys prior to disposal. Therefore, we are not making recommendations for corrective action.

Laptops

During the 2015-16 laptop rollout, individuals under the direction of ISTS staff removed hard drives from laptops returned by users. Our physical inspection of 183 judgmentally-sampled laptops confirmed that the hard drives were removed as noted on the container. After the hard drives were removed, the laptops no longer contained sensitive GAO data and could be disposed.

The removed hard drives were stored in a locked vault within a larger room controlled by badge access. To ensure irreversible removal of all information contained on a hard drive, each hard drive was degaussed through a process that exposed the hard drive to a powerful magnetic field. According to ISTS staff, the degausser's magnetic field was checked prior to each use to ensure that it was operating within the manufacturer's stated parameters. An ISTS employee performed the degaussing procedure or observed an ISTS contractor carrying out the process. Finally, the ISTS staff spot-checked approximately 10 percent of degaussed hard drives.

We tested 141 hard drives and did not identify data on any of them. Specifically, we found that GAO's degaussing process rendered all of the hard drives unusable and thereby unreadable. Further, we also found that GAO's process for removing hard drives from laptops and degaussing the hard drives was effective. Overall, we concluded that GAO policies and procedures for removal of sensitive data from laptops were effectively designed and implemented.

BlackBerrys

During the replacement effort, as users turned in their BlackBerrys, ISTS personnel deactivated them from the BES and transferred the phone numbers to the users' new iPhones. According to ISTS staff, ISTS personnel should have wiped each BlackBerry after the phone number was transferred successfully. Finally, ISTS staff prepared the BlackBerrys for disposal by removing both the battery and back and cataloging each device by Mobile Equipment Identifier (MEID) number using a barcode scanner.

We inserted a fully charged battery in 52 judgmentally-sampled BlackBerrys and made the following overall observations:

- 27 were wiped
- 22 were not wiped
- 3 would not turn on and could not be assessed

While we identified 22 BlackBerrys that were not wiped, GAO's BlackBerrys are protected by device-level encryption and a limit of ten failed password attempts that reduce the risk of unauthorized data retrieval. We also observed that GAO controlled physical access to the devices by storing them in a secure area with access limited to ISTS staff.

Further, GAO has contracted shredding services to dispose of BlackBerrys and other cellular telephones in the past. According to ISTS staff, the current inventory of BlackBerrys will also be shredded once they are all collected. Shredding will render all of the BlackBerrys unusable and thereby unreadable. We concluded that GAO's controls for disposal of BlackBerrys were effective in reducing the risk of unauthorized access to sensitive data.

Appendix I: Objective, Scope, and Methodology

The objective of this audit was to assess GAO's compliance with its policies and procedures regarding media sanitization, and to determine whether laptops and BlackBerrys ready for release outside the agency were appropriately sanitized.

To assess whether GAO's media sanitization policies and practices are appropriate and were being followed, we analyzed GAO's policies and practices and compared them to National Institute of Standards and Technology (NIST) media sanitization standards.[4]

For example, we analyzed the agency's information security policies, procedures, and guidance, including GAO's Information Systems & Technology Services (ISTS) Standard Operating Procedure (SOP) *ISTS-LHM-3 Media Sanitation Process*, ISTS SOP *ISTS-LHM-4 Preparing IT Assets for Excess*, Facilities Management and Services SOP *FMS-PB-17 Excessing Property – Headquarters*, and GAO's degausser procedures.

To supplement our understanding of GAO's media sanitization program and controls, we interviewed staff within ISTS' Customer Relations and Engineering and Operations groups and GAO's Property Branch. We also obtained additional documentation, including: completed custody transfer forms, signed authorizations to excess property, and a contractor's certificate of destruction from a prior disposal of wireless devices.

We tested laptops and BlackBerrys ready for release outside the agency to determine if any readable data was available.

Laptops

We retrieved 426 hard drives that were ready to be excessed. Of that universe, we tested a judgmental sample of 141 hard drives using digital forensic tools to determine if any readable data were available.

In addition, we observed and verified the degaussing process and physically inspected a judgmental sample of 183 laptops identified as having no hard drive to ensure that hard drives were removed.

BlackBerrys

We retrieved 52 of approximately 208 BlackBerrys that were ready to be excessed. We attempted to power on each of the 52 BlackBerrys to determine whether any readable data were available.

Finally, we shared our findings with GAO and obtained oral comments regarding our assessment of its compliance with media sanitization standards, which we incorporated, as appropriate.

[4]NIST, *Guidelines for Media Sanitization*, SP 800-88, Revision 1 (Gaithersburg, Md.: Dec. 2014).

We conducted this performance audit from August 2016 through November 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Major Contributors to This Report

Douglas Carney was the engagement manager for this review.

Appendix III: Report Distribution

U.S. Government Accountability Office

Gene Dodaro – Comptroller General
Patricia Dalton – Chief Operating Officer
Karl Maschino – Chief Administrative Officer/Chief Financial Officer
Susan Poling – General Counsel
Howard Williams Jr. – Chief Information Officer
William Anderson – Controller/Deputy Chief Financial Officer
Adrienne Walker – Director, Program Analysis and Operations
Adebiyi Adesina – Special Assistant to the Controller
Katherine Siggerud – Managing Director, Congressional Relations
Chuck Young – Managing Director, Public Affairs

GAO Audit Advisory Committee

Reporting Fraud, Waste, and Abuse in GAO's Internal Operations

To report fraud and other serious problems, abuses, and deficiencies relating to GAO programs and operations, do one of the following. (You may do so anonymously.)

- Call toll-free (866) 680-7963 to speak with a hotline specialist, available 24 hours a day, 7 days a week.
- Online at: https://OIG.alertline.com.

Obtaining Copies of OIG Reports and Testimony

To obtain copies of OIG reports and testimony, go to GAO's website: www.gao.gov/about/workforce/ig.html.

OIG

Office of Inspector General
U.S. Government Accountability Office