



**INSPECTION REPORT**  
**NUMBER 20-09**

---

**GPO's Electronic Waste (e-waste) Processes and  
Procedures**

**September 10, 2020**

---

### **Questions, Copies, Suggestions**

The Inspections Division, Office of the Inspector General, GPO, prepared this report. If you have questions about the report or want to obtain additional copies, contact the Office of the Inspector General, GPO.

To suggest ideas for or request future inspections of GPO issues, contact the Office of the Inspector General, GPO:

**Telephone:** 1-800-743-7574

**Fax:** 202-512-1352

**e-mail:** [gpoighotline@gpo.gov](mailto:gpoighotline@gpo.gov)

**Mail:** Government Publishing Office  
Attention: Inspector General  
732 North Capitol St. NW  
Washington, DC 20013



*Report violations of law, rules, or agency regulations, mismanagement, gross waste of funds, abuse of authority, danger to public health and safety related to the U.S. Government Publishing Office contracts, programs and/or employees.*

*All reports are made in strict confidence*

**Hotline 1-800-743-7574**

Email: [gpoighotline@gpo.gov](mailto:gpoighotline@gpo.gov)



**Date**

September 10, 2020

**To**

Director,  
U.S. Government Publishing Office

**From**

Inspector General

**Subject:**

Final Report—GPO's Electronic Waste (e-waste) Processes and Procedures 20-09

Enclosed is the subject final report. The Office of the Inspector General (OIG) conducted an inspection of GPO's Electronic Waste (e-waste) Processes and Procedures to evaluate and e-waste accounting, sanitization, and disposal.

We found that GPO has sufficient e-waste accounting policies. However, GPO can improve its oversight of e-waste disposal and accounting once assets are transferred to the contractor. In addition GPO can clarify e-waste related directives and procedures to alleviate confusion over sanitization procedures. Management provided comments and concurred with the finding and recommendations. Management is already taking steps to address the recommendation as shown in Appendix D.

GPO's management and staff were helpful and accommodating throughout this review. If you have any questions or comments about this report, please do not hesitate to contact Nathan Deahl, Assistant Inspector General for Inspections, [ndeahl@gpo.gov](mailto:ndeahl@gpo.gov), or me at [mleary@gpo.gov](mailto:mleary@gpo.gov).

A handwritten signature in black ink, appearing to read 'M. Leary'.

MICHAEL P. LEARY  
Inspector General

## RESULTS IN BRIEF

### What We Did

The Office of the Inspector General assessed the effectiveness of GPO's e-waste disposal program, procedures, and processes. The inspection team focused on GPO's procedures for e-waste accounting and sanitization.

### What We Recommend

Our report contains two recommendations designed to improve oversight of the e-waste disposal contract and align GPO practices with its directives and procedures. The recommendations focus on e-waste related directives and call on GPO to periodically spot check its e-waste vendor.

## Inspection of GPO E-Waste Procedures Governing Accounting and Sanitization

### What We Found

**GPO can improve its oversight of e-waste disposal and accounting once assets are transferred to the contractor. In addition GPO can clarify e-waste related directives and procedures to alleviate confusion over sanitization procedures.**

In the past, GPO physically verified e-waste destruction by the contractor at their facility. GPO has not done so since 2017 due to organizational changes that limited the manpower associated with e-waste oversight. As a result, since 2017, the Chief Information Officer's (CIO's) organization has not spot checked e-waste destruction and thus GPO is at an increased risk for both fraud and exposure of sensitive information.

GPO has e-waste accounting directives as well as practices that govern how e-waste is secured and sanitized. However, some of the practices do not align with policy. For example, according to GPO policy, Business Units (BUs) are required to have procedures to sanitize sensitive information; however, of the 14 BUs who responded to our data call, none had procedures written for their handling of e-waste. Rather, they stated that they follow the CIO's practices (that of turning in equipment to the Information Technology (IT) BU). Further, there was confusion in the IT BU as to whether hard drives were sanitized prior to destruction and release to vendor control. GPO policy has not been updated to reflect its current destruction practices. GPO can alleviate confusion by clarifying their directives and procedures to align with their current practices for hard drive sanitization.

# CONTENTS

<b>Introduction</b>	1
Background	1
Objectives	6
Prior Evaluation Coverage	6
Criteria	6
<b>Inspection Results</b>	7
Finding 1. GPO can improve its oversight over e-waste disposal and accounting once assets are transferred to the contractor. In addition GPO can clarify e-waste related directives and procedures to alleviate confusion over sanitization procedures.	7
<b>Appendixes</b>	11
Appendix A. Table of Recommendations	11
Appendix B. Scope and Methodology	12
Appendix C. Abbreviations	13
Appendix D. Management Comments	14
Appendix E. Report Distribution	15

## INTRODUCTION

The Office of the Inspector General (OIG), Inspections Division, reviewed GPO Information Technology (IT) end user asset management, specifically the disposal of assets no longer useful to GPO; this practice is commonly known as electronic waste (e-waste) disposal. Based on the results, we made two recommendations (see appendix A); scope and methodology are presented in appendix B.

### **Background**

We initiated this review to understand GPO's procedures for handling e-waste, including its policies, procedures, and methods for securing/sanitizing e-waste. The review covered the period of time from calendar years 2018–2019. This was an ad hoc project added to the FY 2020 Audit and Inspection plan. This inspection supports GPO's 2<sup>nd</sup> strategic goal to enhance access to Federal Government information by using a comprehensive IT security posture.

### ***The Issue***

GPO's mission is to keep America informed as the official, digital, and secure source for producing, preserving, and distributing official Federal Government publications and information products for Congress, Federal agencies, and the American public. GPO makes use of a variety of electronic equipment to perform its mission such as laptops, workstations, servers, cellphones, and copiers. The GPO CIO, and Director of the IT BU oversee the lifecycle of IT equipment from procurement to disposal. This equipment includes but is not limited to: desktop computers, laptops, printers, tablets, mobile devices, scanners, facsimile equipment, photocopiers, multi-functional devices, etc.

### ***What is E-Waste?***

"E-waste", "electronic waste", "e-scrap" and "end-of-life electronics" are terms often used to describe used electronic equipment that are nearing the end of their useful life, and are discarded, donated, or recycled. Though "e-waste" is the commonly used term, the Environmental Protection Agency (EPA) considers e-waste to be a subset of used electronics and recognizes the inherent value of these materials that can be reused, refurbished or recycled to minimize the actual waste that might end up in a landfill or improperly disposed in an unprotected dump site either in the U.S. or abroad.

### ***Why is it Important to Govern E-Waste?***

In addition to the monetary value of recycled equipment, an effective electronic disposal process includes tracking, securing, and sanitizing. Sanitization is a process where data is removed from media or the media is permanently destroyed. These steps are critical for protecting sensitive data against unauthorized disclosure. E-waste

is also of interest to parties seeking sensitive information on disposed electronic media.

In addition to sensitive information that may reside on e-waste, GPO defines a Sensitive System as one that requires additional protections or controls due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information associated with or processed by the system. The term includes information whose improper use or disclosure could adversely affect the ability of the GPO to accomplish its mission, e.g., proprietary information, or information about individuals requiring protection under GPO privacy policies. E-waste sanitization, or media sanitization, is a general term referring to the actions taken to render data written on the electronic media into an unrecoverable state by both ordinary and extraordinary means. The application of effective sanitization techniques are a critical aspect of ensuring that sensitive data is effectively protected by an organization against unauthorized disclosure. Protection of information, in all forms, is paramount. A common type of sensitive information is Personally Identifiable Information (PII) of GPO employees, defined below.

### ***Personally Identifiable Information (PII)***

Broadly, PII is “information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.” (OMB Memorandum 07-16). Other specific examples of PII include, but are not limited to:

- a) Personal identification number, such as passport number, driver’s license number, taxpayer identification number, or financial account or credit card number;
- b) Address information, such as street address or personal email address; and
- c) Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), fingerprints, handwriting, or other biometric image or template data (e.g., retina scans, voice signature, facial geometry).

Again, the application of effective sanitization techniques is a critical aspect of ensuring that sensitive data is effectively protected by an organization against unauthorized disclosure.

### ***The GPO E-Waste Disposal Process***

GPO has internal disposal procedures and contracts for the physical destruction of hardware such as computers, servers, and laptops. GPO also has a second contract for the lease of copiers and scanners, which includes terms for hard drive encryption and

sanitization. Moreover, GPO has an iPhone standard operating procedure and practices that include a step for “wiping” iPhones.<sup>1</sup>

The steps of the computer replacement process related to e-waste are described below. The process at GPO originates with a computer replacement request from an end user (GPO employee). End users submit an IT ServiceHUB ticket. An IT technician acts on the ticket request and will then physically retrieve the old equipment from the customer, and eventually remove the hard drive if the computer is to be retired. The technician updates the IT Service Hub ticket to include the following information about the computer: a service tag number, a hard drive serial number (only if machine is being retired), and the make and model number. We were informed this overall process leads to a hard drive re-image<sup>2</sup> for the computer that will be turned over to IT. The reimaging includes sanitization of the old computer hard drive. The computer and hard drive once separated from the computer are finally placed in a receptacle in a storage room that is located across the hallway from the IT Service Desk space, Figure 1.

**Figure 1 – Room C-843 Hard Drives removed from computers**

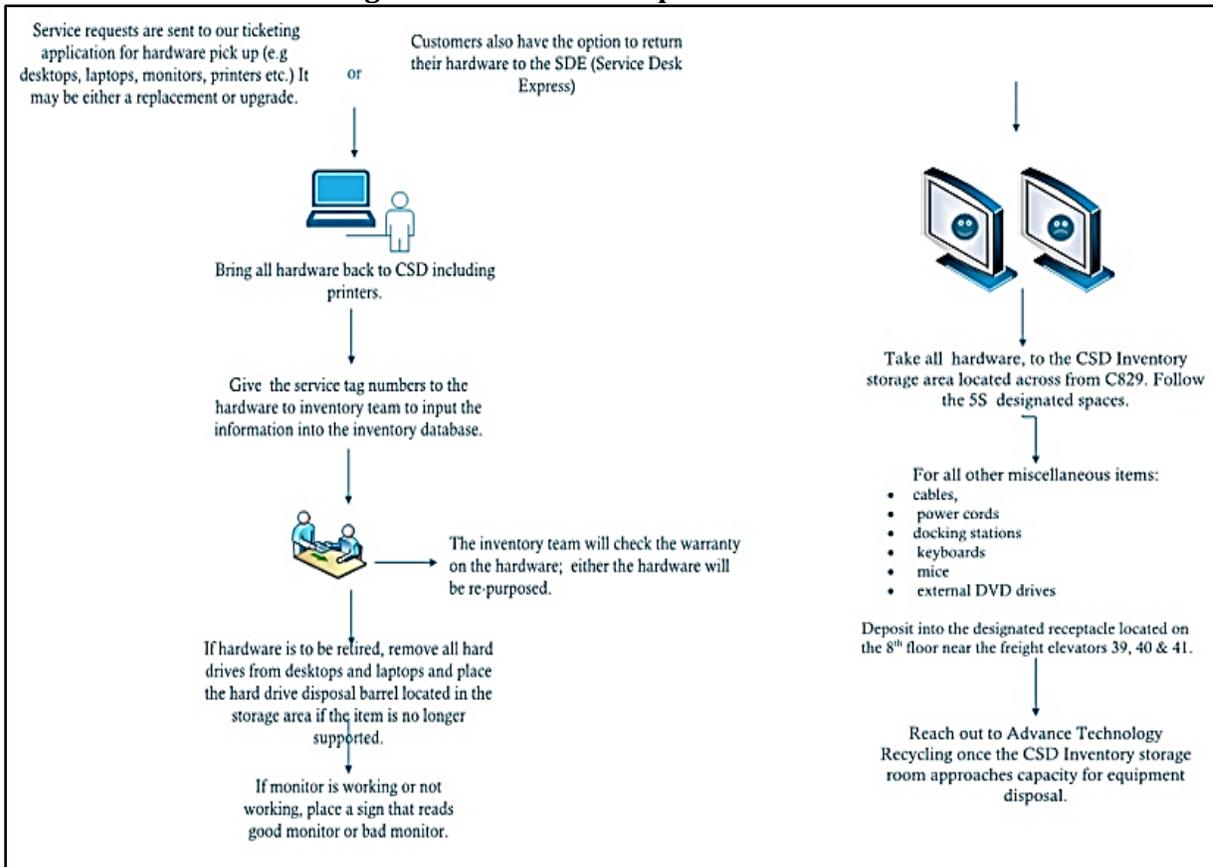


<sup>1</sup> Due to the COVID-19 operating status, we were unable to personally verify the copier hard drive encryption or sanitization controls process and the process for iPhone wiping; however this did not affect our finding.

<sup>2</sup> An “image” is a computer file containing the encapsulated components of an operating system and applications. To “re-image” is to reapply the operating system to the computer overwriting the previous files and operating system.

The following graphic depicts the hardware disposal process that was described above, Figure 2.

**Figure 2 - Hardware Disposal Process<sup>3</sup>**



<sup>3</sup> Computer Service Desk (CSD).

## Hardware Disposal Contract

GPO contracts the hardware disposal to Advanced Technology Recycling (ATR), which is an electronic recycling company. The contractor is periodically tasked by GPO to pick up e-waste. For the calendar years 2018 and 2019, GPO had the contractor pick up a total of 750 assets listed by equipment type in Table 1 below.

**Table 1. Contractor E-Waste Asset Disposal**

<b>Equipment Type</b>	<b>Number</b>
Laptop	194
Computer / PC	161
Hard Drive	144
LCD Monitor	106
Printer / Copier	103
Thin Client	15
Miscellaneous / Other	8
Keyboard/Mouse/Peripheral	7
Networking / Phones	4
Server	4
LCD TV	3
CRT / Monitor	1

According to our review of the contract and our interviews with GPO's subject matter experts (SMEs), the contractor takes the e-waste to its facility to inventory, process, and destroy. However, the interviewed SMEs had a disparate understanding of hard drive sanitization prior to the contractor taking possession of the equipment. For example, some GPO IT Services' personnel stated that all hard drives are physically destroyed by the contractor without first being sanitized (this is the actual process which we verified). However, other individuals stated that all hard drives are sanitized prior to delivery to contractor as the GPO Directive 825.41A, *Privacy Program: Protection of Personally Identifiable Information (PII)*, June, 12 2015, states. We discuss this in more detail below. We did confirm that the contractor creates a certificate of disposal for all items collected from GPO. GPO receives the electronic certificate of disposal for all items recycled by the contractor. The contractor's certification includes the following footnote:

This electronic report constitutes final Asset Disposition and should be considered an electronic "Certificate of Destruction/Recycling" for equipment contained within this report. Advanced Technology Recycling (ATR - The contractor) assumes all responsibility for the recycling/reclamation/re-marketing efforts as they relate to this equipment and we hereby certify to adhere to all Local/State/Federal guidelines as they relate to Electronic or Universal Solid Waste Management.

It was our intention to visit the contractor site to verify GPO's e-waste disposal, however, due to the COVID-19 operating status we could not witness the destruction of e-waste.

## Objectives

Our overall objective was to determine the effectiveness of GPO's e-waste processes and procedures. The inspection sub-objectives were to review GPO procedures for e-waste accounting as well as its practices for securing/sanitizing e-waste.

## Prior Evaluation Coverage

GPO OIG issued an audit of Control and Accountability of Laptop Computers on December 6, 2010. The objective of that audit was to determine whether GPO (1) could account for all agency laptop purchases, and (2) had adequate controls in place that would prevent the loss or theft of laptops. All recommendations from that audit were closed.

## Criteria

We used the following sources as criteria during this inspection. A further breakout of the criteria as they relate to specific findings are included in that finding's section.

- GPO Directive 705.29B, *Information Technology End User Asset Management (IT Equipment)*, December 10, 2019.
- GPO Directive 825.41A, *Privacy Program: Protection of Personally Identifiable Information (PII)*, June 12, 2015.
- GPO Directive 825.33B, *Information Technology (IT) Security Program Statement of Policy*, May 24, 2011.
- Contract Number 040ADV-19-P-9494, *Advanced Technology Recycling*, Award date September 27, 2019.
- Contract Number: B951-M, Task Order Number: 20159 R-1, *Lease of Multi-Function Devices*, August 7, 2017.
- National Institute of Standards & Technology (NIST) SP 800-88 Rev 1, *Guidelines for Media Sanitization*, December 2014.
- GPO iPhone Disposal Standard Operating Procedure (SOP), May 5, 2020.
- GPO CSD Policy and Procedures for Computer Replacement version 3, undated.
- GPO Hardware Disposal Procedure, undated
- Memorandum from the Director of GPO, *Information Requested Supporting E-Waste Inspection (SP-20-02)*, April 28, 2020.

## INSPECTION RESULTS

### **Finding 1. GPO can improve its oversight of e-waste disposal and accounting once assets are transferred to the contractor. In addition GPO can clarify e-waste related directives and procedures to alleviate confusion over sanitization procedures.**

In the past, GPO physically verified e-waste destruction by the contractor at their facility. GPO has not done so since 2017 due to organizational changes that limited the manpower associated e-waste oversight. As a result, since 2017, the CIO's organization has not spot checked e-waste destruction and thus GPO is at an increased risk for both fraud and inadvertent exposure of sensitive information.

GPO has e-waste accounting directives as well as practices that govern how e-waste is secured and sanitized. However some of the practices do not align with policy. For example, according to GPO policy, BUs are required to have procedures to sanitize sensitive information; however, of the 14 BUs who responded to our data call, none had procedures written for their handling of e-waste. Rather, they stated that they follow the CIO's practices (that of turning in equipment to the IT BU). GPO policy has not been updated to reflect its current destruction practices. GPO can alleviate confusion by clarifying their directives and procedures to align with their current practices for hard drive sanitization.

#### **Criteria**

- GPO Directive 705.29B, *Information Technology End User Asset Management (IT Equipment)*, states that the IT BU manages the inventorying, tracking, removing, and securely disposing of the unused equipment, which includes, but is not limited to: desktops, laptops, printers, tablets, mobile devices, scanners, facsimile equipment, photocopiers, and multi-functional devices. Additionally, the equipment is to be securely sanitized prior to being disposed. Further, IT Operations is to perform an annual audit of all end-user IT equipment.
- GPO Directive 825.41A, *Privacy Program: Protection of Personally Identifiable Information (PII)*, states that all computing equipment that once contained PII must be sanitized before being transported offsite or returned to the IT BU for disposition. Each BU is required to develop comprehensive procedures for identifying and protecting the confidentiality of PII under its control, consistent with this directive and in coordination with the Privacy Officer.
- GPO Directive 825.33B, *Information Technology (IT) Security Program Statement of Policy*, states all GPO systems that have a computer hard disk, including but not limited to, copiers, multifunction devices, and cell phones/Blackberries, shall be sanitized (which ensures erasure of all digital data), prior to the system being retired, or returned to the vendor in cases where the data is not required to perform repair.

- GPO iPhone Disposal SOP requires the following: “All wireless equipment must be returned to GPO/IT for employees leaving the agency or when a replacement/upgrade is required. The iOS device is wiped of all GPO user data and the...ID is disassociated from the device...The device is released...to clear the GPO image from the device...The device is deleted...the profile is removed if the user is leaving the agency.”
- Contract Number: B951-M, Task Order Number: 20159 R-1, Lease of Multi-Function Devices, includes a task order with requirements for the devices to have hard drive encryption as well as Data/Image Overwriting that will electronically shred information stored on the hard disk as part of routine job processing.
- Contract Number GS-10F-134BA, B&K Technology Solutions Inc. d/b/a Advanced Technology Recycling, specifies that “...all data residing on the hard drives of desktops, laptops, printers, and copiers shall be wiped and or destroyed in accordance with media sanitations standards outlined by the NIST SP 800-88 and DoD Standard 5220.22M.”
- NIST SP 800-88 Rev 1, Guidelines for Media Sanitization, defines: “Clear, Purge, and Destroy are actions that can be taken to sanitize media. The categories of sanitization are defined as follows: Destroy renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data.”
- The GPO CSD Policy and Procedures for Computer Replacement version 3, has procedures for reimaging hard drives.
- Memorandum from the Director of GPO, Information Requested Supporting E-Waste Inspection (SP-20-02), states that BUs follow the CIO e-waste process.

### **Improve Contractor Oversight with Spot Checks**

GPO last witnessed the contractor physically destroying e-waste, at the contractor facility, in 2017. In addition, the CIO’s staff stated they had not witnessed the destruction procedures with the current vendor, ATR. According to those we interviewed, the proximate cause of this condition was that when the e-waste management functions were transferred, the incumbent manager’s workload (between already present and acquired responsibilities) prevented the previous level of oversight. As a result, since 2017, the CIO’s organization has not spot checked e-waste destruction and thus GPO is at an increased risk for both fraud and inadvertent exposure of sensitive information.

### **GPO’s E-Waste Procedures Need Improvement to Alleviate Confusion**

As discussed in the introduction of this report, GPO BUs use the IT BU’s disposal practices of turning in old equipment to the IT BU in accordance with GPO Directive 705.29B. All of the BUs who responded to our data-call (14) turn in their excess electronics to the IT BU

without individually sanitizing their information. However, according to GPO Directive 825.41A, all computing equipment that once contained PII must be sanitized before being transported offsite or returned to the IT BU for disposition. Moreover that policy states that the BUs are required to develop comprehensive procedures for identifying and protecting the confidentiality of PII under its control, consistent with this directive and in coordination with the Privacy Officer. We confirmed that the BUs do not have individual procedures written as required by GPO Directive 825.41A. Thus, GPO has two overarching directives in conflict, GPO Directive 705.29B and Directive 825.41A. The existence of two policies with contradictory information leads to confusion. In fact, personnel within the IT BU itself had conflicting accounts of the sanitization procedures discussed below.

### ***Sanitization Clarification***

Through our interviews, we discovered individuals within the IT BU had differing views on the sanitization requirements in order to retire hard drives. One view was that all hard drives are to be sanitized prior to disposal of and the other is that the contractor's destruction of hard drives remediates the need for internal GPO sanitization. GPO Directive 705.29B states that the IT BU manages the inventorying, tracking, removing, and securely disposing of the unused equipment, which includes, but is not limited to: desktops, laptops, printers, tablets, mobile devices, scanners, facsimile equipment, photocopiers, and multi-functional devices. Additionally, the equipment is to be securely sanitized prior to being disposed. GPO Directive 825.33B, states all GPO systems that have a computer hard disk shall be sanitized (which ensures erasure of all digital data) prior to the system being retired, or returned to the vendor in cases where the data is not required to perform repair.

Through our interviews we learned that GPO's IT disposal practice does not match its policy. We found that GPO IT does not sanitize hard drives prior to processing them out of GPO. Instead, hard drives are simply destroyed by the contractor once computers have reached the end of their useful life at GPO. It is GPO's assertion that given their personnel resources, this is the safest course to take. Destruction is an acceptable control for media sanitization as noted in NIST Special Publication 800-88 Revision 1, which states:

Clear, Purge, and Destroy are actions that can be taken to sanitize media, defined below:

“Destroy” renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data.

Although GPO is in compliance with Federal policy for media sanitization, its directives do not align with its practices. Moreover, as stated earlier, GPO runs the risk of potential fraud, theft, and inadvertent release of sensitive information because GPO is not verifying that the contractor is destroying the information. In order to improve GPO's e-waste disposal program we make the following recommendations.

## **Recommendations**

For the Director of GPO:

**Recommendation 1:** GPO should update its directives to align with its practices for hard drive sanitization and BU procedures.

**Recommendation 2:** GPO should perform periodic verification of destruction of e-waste at its contractor facility.

Management concurred with the findings and recommendations. Management comments are included in Appendix D.

## Appendix A. Table of Recommendations

Recommendation	Management Response	Status	Description of Benefits
<b>For the Director of the Government Publishing Office</b>			
<p>GPO should update its directives to align with its practices for hard drive sanitization and Business Unit procedures.</p>	<p>Management Concurred. To address inconsistencies / gaps in current policies as they apply to eWaste disposal, the Office of the CIO has created a new agency wide directive entitled "Information Technology Electronic Equipment Disposal (e-Waste) Policy". The policy is being staffed for approval.</p> <p>Once the policy is approved the OIG will review for closure.</p>	<p>Open</p>	<p>Nonmonetary – Improve program results</p> <p><i>Practices should align to policy.</i></p>
<p>GPO should perform periodic verification of destruction of e-waste at its contractor facility.</p>	<p>Management Concurred. GPO's Office of the CIO will resume the practice of spot checking the destruction of items by its vendor to further reduce the risk of fraud and exposure of sensitive information.</p> <p>Once GPO begins spot checks again, the OIG will evaluate this recommendation for closure.</p>	<p>Open</p>	<p>Nonmonetary – Improve program results</p> <p><i>Periodic verification should ensure the contractor is performing the contract.</i></p>

## **Appendix B. Scope and Methodology**

### **Scope**

- The OIG inspection team reviewed GPO IT end user asset management, specifically the disposal of assets no longer useful to GPO. We also assessed whether GPO had procedures for e-waste accounting and electronic media sanitization.
- The GPO Chief Information Officer was the primary entity in GPO reviewed during this inspection. We collected data from all the GPO Business Units regarding their procedures as they relate to the GPO Privacy Program to review sections applicable to e-waste.

### **Methodology**

- We reviewed GPO directives applicable to e-waste, as well as related standard operating procedures, contracts, and task orders.
- We interviewed the Chief Information Officer and BU staff.
- We were limited in our ability to witness GPO practices for e-waste due to the COVID-19 telework operating environment. The GPO contract recycler was also not available to speak with the OIG due to the COVID-19 operating state and limited staff.
- No pertinent information was omitted from the report because it was deemed privileged or sensitive.
- This inspection was conducted in accordance with the Quality Standards for Inspections and Evaluations of the Council of the Inspectors General on Integrity and Efficiency, January 2012.

## **Appendix C. Abbreviations**

ATR	Advanced Technology Recycling
BU	Business Unit
CIO	Chief Information Officer
COVID-19	Corona Virus Disease, 2019
CSD	Computer Service Desk
E-waste	Electronic Waste
EPA	Environmental Protection Agency
OIG	Office of the Inspector General
IT	Information Technology
NIST	National Institute of Standards & Technology
PII	Personally Identifiable Information
SDE	Service Desk Express
SME	Subject Matter Expert

# Appendix D. Management Comments

<b>MEMORANDUM</b>		
SUBJECT	<u>CIO Response to OIG eWaste Inspection Report SP-20-02</u>	DATE <u>9/04/20</u>
REPLY TO ATTENTION OF	<u>Office of the Chief Information Officer (CIO)</u>	<u>Sam Musa</u>
TO	<u>Office of the Inspector General</u>	
<p>GPO's Office of the CIO concurs with the findings of the Inspector General's eWaste Inspection Report SP-20-02 and offers the responses detailed below:</p>		
<p><i><b>OIG Recommendation 1:</b> GPO should update its directives to align with its practices for hard drive sanitization and BU procedures.</i></p>		
<p><b>CIO Response to Recommendation #1:</b> To address inconsistencies / gaps in current policies as they apply to eWaste disposal, the Office of the CIO has created a new agency wide directive entitled "Information Technology Electronic Equipment Disposal (e-Waste) Policy". The proposed directive has been reviewed and approved by GPO's Office of General Council and is awaiting the signature of the agency director.</p>		
<p>Additionally, policies such as GPO Directive 825.41A, Privacy Program: Protection of Personally Identifiable Information (PII); GPO Directive 705.29B, Information Technology End User Asset Management (IT Equipment); GPO Directive 825.33B, Information Technology (IT) Security Program Statement of Policy, will be updated for consistency with the new eWaste directive.</p>		
<p><i><b>OIG Recommendation 2:</b> GPO should perform periodic verification of destruction of e-waste at its contractor facility.</i></p>		
<p><b>CIO Response to Recommendation #2:</b> GPO's Office of the CIO will resume the practice of spot checking the destruction of items by its vendor to further reduce the risk of fraud and exposure of sensitive information. Spot checks will be resumed toward the easing of the current nationwide pandemic by either:</p>		
<ul style="list-style-type: none"><li>a) Providing GPO IT personnel to accompany the transport of agency eWaste computer systems and hard drives to the vendor's processing plant to witness their destruction, or</li><li>b) Arranging for the onsite destruction of eWaste materials by the vendor at GPO Headquarters.</li></ul>		
<p>The next spot check of the vendor's eWaste destruction process is tentatively scheduled for the third week of September (2020) at which time the vendor will perform onsite destruction of hard drives at GPO Headquarters. This operation will be witnessed by authorized GPO IT personnel.</p>		
<p>U.S. GOVERNMENT PUBLISHING OFFICE   Keeping America Informed   OFFICIAL   DIGITAL   SECURE 732 North Capitol Street, NW, Washington, DC 20401-0001   <a href="http://www.gpo.gov">http://www.gpo.gov</a>   <a href="http://www.facebook.com/USGPO">www.facebook.com/USGPO</a>   <a href="http://twitter.com/USGPO">twitter.com/USGPO</a> Form 731 7/15</p>		

## **Appendix E. Report Distribution**

Director

Deputy Director

Acting Chief of Staff

Chief Information Officer