BASIC PRIVACY TRAINING

Fiscal Year 2024
(PII – 101)

Mandatory Annual Training for all GPO Employees and Contractors

Prepared by:

GPO Privacy Office
Information Technology

GPO

What is a Privacy?

Privacy – is the right of individuals to determine for themselves -

When, how, and to what extent information about them is collected and disseminated to others.

Individuals in this context could be an employee, a contractor, a customer, a vendor, or the public.

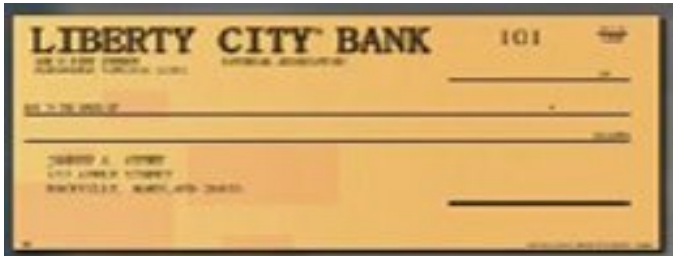
Today, ***privacy has become a core value*** of democratic societies and being treated as an essential aspect of freedom and human dignity.

Privacy, in addition to Information Security, also requires an organization to consider:

- Safeguarding interests of individuals and extending them rights in their data collection, maintenance, use, and disposition.
- Informing employees regarding collection of their personal information (including health information), and making them aware of the purpose, why their PII, is being collected, due process, and mitigation options in case of a breach
- Giving them choices (where applicable). Yes, individuals have right to ask for corrections
- As the Internet and social media explode, the privacy domain is also expanding. Factually, it now expands to employees' Internet activity, visits to medical unit, telephone conversations, emails, and workspace.

Refer to GPO Directive 825.33C

What is PII?



OMB Memorandum 17-12:

"Personally Identifiable Information (PII) is *information which can be used to distinguish or trace an individual's identity... when used alone, or when combined with other personal or identifying information".*

GPO Directive 825.41B:

"PII information which can be used to distinguish or trace an individual's identity, such as their name, Social Security Number (SSN), biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual".

GPO

What is PII? (Continue…)

Here is a partial list of PII:

- Social Security Number, full or truncated
- Birth date, place of birth – Citizenship and legal status
- Educational or employment records
- Financial transactions, direct deposit information, credit card or bank account numbers
- Medical information
- Criminal history that contains name, payroll number, social security number
- Name combined with date of birth or place of birth
- Other identifying particulars, such as a finger or voice print or a photograph
- Spouse information, marital status, and child information

Protected Health Information – PHI

PHI – call it Protected Health Information, Personally Identifiable Health Information, or just Personally Identifiable Information (PII) that contains an individuals' private health information. Collectively, PII & PHI are called PII.

PHI generally shows up in the following*:

- Medical Folder (paper or electronic) contains health, biometric or disability information, as well as health Plan (Insurance) account numbers, emergency contact information.
- Correspondence from doctor
- Lab results (Blood test reports/Radiology films & reports/Physicians' notes)
- Phone records/Emails/Fax
- Medical Unit Visit records (in any form)
- Computer/Tablet/Phone/Electronic Storage

The Health Insurance Portability and Accountability Act identifies (HIPAA) promulgates standards and/or rules to promote and monitor PII/ PHI compliance.
Please note: GPO takes PHI seriously and embraces spirit of HIPPA however, HIPPA as a law does not apply to GPO.

** OMB Memorandum M-17-12*

GPO

PII categories: Sensitive PII

PII (hard copy or digital) can be categorized as sensitive or non-sensitive, based on their potential risk of harm.

For example, SSN, or medical history is generally considered more sensitive than an individual's phone number or ZIP code.

Non-sensitive data elements in conjunction with the identity of an individual, can at times also be considered sensitive, such as, a simple list of employees when includes performance ratings may be classified as sensitive.

Sensitive PII include, but not limited to*:

- SSN, full and truncated
- Birth date/place, citizenship and legal status
- Name (other names used), mother's maiden name
- Driver License, Passport, or Alien Number
- Financial information: credit cards, deposits, etc.
- Medical, biometric or disability information
- User IDs/Passwords
- Emergency contact information
- Gender, race/ethnicity - religious preference
- Spouse, marital status, and child information
- Criminal or employment history
- Security clearance, military records

OMB Memorandum M-17-12

GPO

PII categories: Non-Sensitive PII

Non-Sensitive PII can be transmitted electronically without protection because they are not considered sufficiently sensitive to require protection.

Non-Sensitive PII include, but are not limited to:

- Personal email address
- User IDs
- Mailing and home address
- Home and personal cell telephone numbers
- Emergency contact information
- Resumes that do not include an SSN or where the SSN is redacted
- General background information about individuals found in resumes and biographies
- Position descriptions and performance plans without ratings

GPO

Do we know our PII is at risk all the time…

Data breaches continue to have become more and more costlier for oraganizations

The 2023 IBM reports the average data breach cost has increased to $4.45 million ($165 per record), with data breaches in the United States being the costliest, at an average of $9.48 million.

Cost to handle Data breaches has increased by 15% annually, since 2020.

Recent 2022-2023 PII breaches:

Twitter Data Breach - Email addresses belonging to around 200 million Twitter users were being sold on the dark web for as little as $2. Even though the flaw that led to this leak was fixed in January 2022, the data is still being leaked by various threat actors.

US House of Representatives Data Breach: A breach through a healthcare provider that affected up to 170,000 people. The data has been put up for sale online. A report said, the FBI is thought to have already purchased it as part of their investigation.

CMS.gov - The Department of Health and Human Services (HHS) and the Centers for Medicare & Medicaid Services (CMS) reported a PII breach that impacted 612,000 current Medicare beneficiaries.

Many Privacy Incidents continue to impact millions of federal and private employees.

GPO

Do we know our PII is at risk all the time… (Continue)

Country	Fullz price on dark web (average, US$)
USA	$8
UK	$14
Turkey	$14
Israel	$14
China	$15
Singapore	$15
Canada	$15
Australia	$15
New Zealand	$20
UAE	$25
Japan	$25
Europe	$25

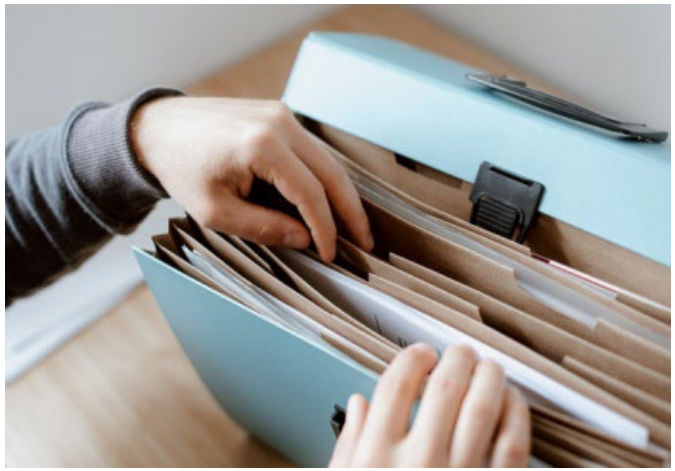
Cybercriminals sell personal information of the US citizens on a dark web. Full credentials of one person - SSN, name, DOB, etc. was priced $8 in 2021*.

Comparitech reports about 40+ dark web marketplaces that sells stolen identities, credit cards and hacked PayPal accounts.

* Security Magazine | The top data breaches of 2021

Price of "Fullz", which is the full credentials (SSN, name, DOB etc.) Source: Comparitech.

GPO Records Management, Private Records, & PII



GPO records (electronic or paper) can also contain PII or PHI, and therefore are private records.

GPO's commitment to privacy extends to GPO Records Management Program (RMP), regardless whether records are in:

- **Possession of Business Units**
- **Records Management warehouse**
- **Records' expungement area**

The GPO Privacy Office in close cooperation with RMP ensures safeguards to protect PII are implemented for both GPO's electronic and paper records.

.

GPO e-mail can also be a Private Record

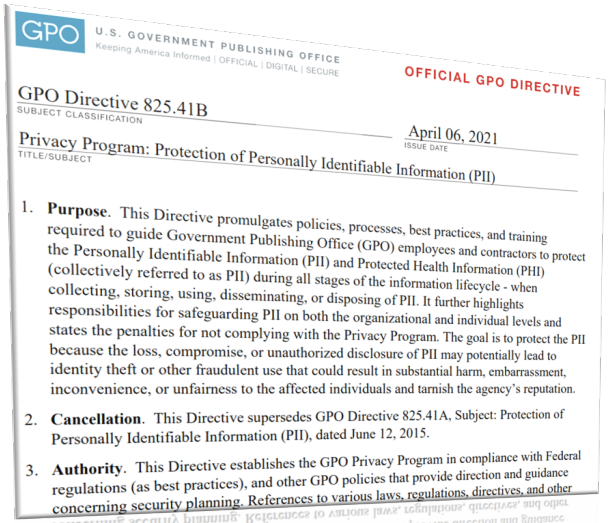
Email may also be treated like any other record, in which GPO business information is created, transmitted, received, or maintained in an electronic format.

Email becomes a private record when it contains any personal, health, financial, or sensitive information belonging to GPO employee, contractor, or other sensitive business information.

Contact GPO Records Officer or your immediate supervisor if your position will require you to maintain GPO personal or private records.

Note - the **content** is what is important (paper vs. electronic is irrelevant).

GPO Privacy Program



GPO U.S. GOVERNMENT PUBLISHING OFFICE
Keeping America Informed | OFFICIAL | DIGITAL | SECURE

OFFICIAL GPO DIRECTIVE

GPO Directive 825.41B
SUBJECT CLASSIFICATION

April 06, 2021
ISSUE DATE

Privacy Program: Protection of Personally Identifiable Information (PII)
TITLE/SUBJECT

1. **Purpose**. This Directive promulgates policies, processes, best practices, and training required to guide Government Publishing Office (GPO) employees and contractors to protect the Personally Identifiable Information (PII) and Protected Health Information (PHI) (collectively referred to as PII) during all stages of the information lifecycle - when collecting, storing, using, disseminating, or disposing of PII. It further highlights responsibilities for safeguarding PII on both the organizational and individual levels and states the penalties for not complying with the Privacy Program. The goal is to protect the PII because the loss, compromise, or unauthorized disclosure of PII may potentially lead to identity theft or other fraudulent use that could result in substantial harm, embarrassment, inconvenience, or unfairness to the affected individuals and tarnish the agency's reputation.
2. **Cancellation**. This Directive supersedes GPO Directive 825.41A, Subject: Protection of Personally Identifiable Information (PII), dated June 12, 2015.
3. **Authority**. This Directive establishes the GPO Privacy Program in compliance with Federal regulations (as best practices), and other GPO policies that provide direction and guidance concerning security planning. References to various laws, regulations, directives, and other

GPO Privacy Program Directive 825.41B states federal regulations, guidance, and best practices to handle and safeguard privacy data at GPO.

GPO Privacy Program highlights the appropriate PII protection measures, privacy compliance requirements, and handling privacy incidents. It further requires,

- Develop privacy compliance documents for each PII containing IT system
- Provide privacy training to employees and contractors, make them aware of the best practices, and ensure they understand the implications of not following the guidelines published in this Directive
- Any GPO system that collects or publishes public PII shall redact PII or receive the written consent of the data provider prior to publishing PII.
- Notify the receiver(s) that they are expected to continue to protect the data using encryption or comparable controls and to immediately report any actual or suspected loss of integrity.

GPO

Best Practices: Handling PII

If you collect PII, you must protect it. Think PRIVACY when handling PII. These are general safeguarding principles for sensitive PII (hard copy or electronic).

Sensitive PII at rest:

- ✓ Protect it by identifying it as “Sensitive PII”
- ✓ Label it as a “For Official Use Only”
- ✓ Don’t keep it longer than needed
- ✓ Keep it in encrypted format and enforce access control mechanism
- ✓ Users must have a business need to remotely access PII on a GPO network or system. Such access is permitted only in conformity with GPO IT Directive 825.35D.
- ✓ Do not leave it unattended on display screen, desks, printers. Keep it in a locked and secured area, when not in use
- ✓ If you happen to see unprotected document containing sensitive PII, inform your supervisor immediately

Best Practices: Handling PII (Continue)

Never email sensitive PII to a personal email account. Disclose it only within authorized people who “need to know”.

When transferring PII containing hard copy records to Records Management, you are required to:

1. Fill the Form 1350 (available on GPO Intranet) and include all PII items in the PII column.
2. Ensure a copy of filled 1350 is included in each box.
3. Ensure boxes are transferred securely.

Disclosing and disposing sensitive PII:

- ✓ Do not post it on the GPO Intranet, the Internet (including social networking sites), shared drives, or multi-access calendars that can be accessed by individuals who do not have an official “need to know”
- ✓ Encrypt PII contained email before sending either internally or externally. Give decryption code to recipient by phone call, or in another email. Do not convey passwords through voicemail.
- ✓ Don’t download PII on external storage that does not provide the GPO
- ✓ Transport it physically between approved locations and with prior authorizations.

Best Practices: Handling PII (Continue)

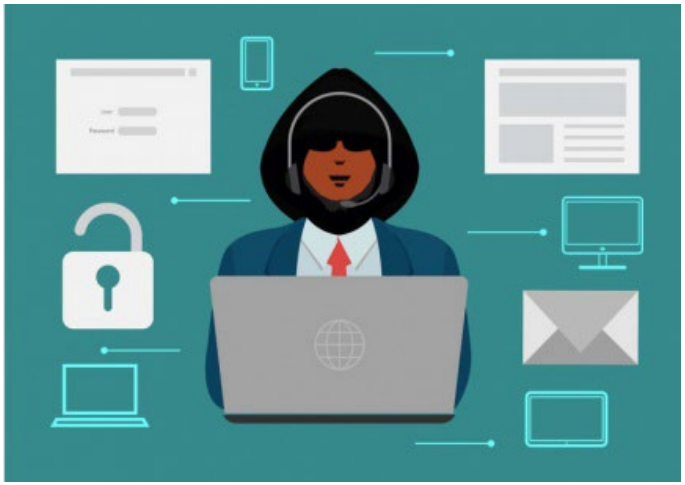
Use only GPO-approved portable electronic device and encrypt the PII data in this device.

Do not leave portable electronic devices in a car. If it is stolen or lost, report it as a lost asset following your reporting procedures

- ✓ Transmit it either in person or in an opaque container using First Class, Priority Mail, or a traceable commercial delivery service like UPS, the USPS, or FedEx
- ✓ Avoid faxing it. If you must use fax, contact the recipient directly to confirm receipt. Always use a cover sheet.
- ✓ When a system containing PII is disposed of, the PII must be securely expunged with a log maintained of expunging activity.
- ✓ If the PII-containing device (BU management informs IT Service Hub of the presence of any PII) is either being retired, disposed of, changed ownership, or sent for repairs, the GPO IT Operations Division ensures the PII at this equipment becomes permanently non-retrievable by any means.
- ✓ All PII containing paper records shall be shredded at a GPO-approved shredding facility and witnessed either by a Federal employee or authorized contractor employee.

GPO

Privacy related security events



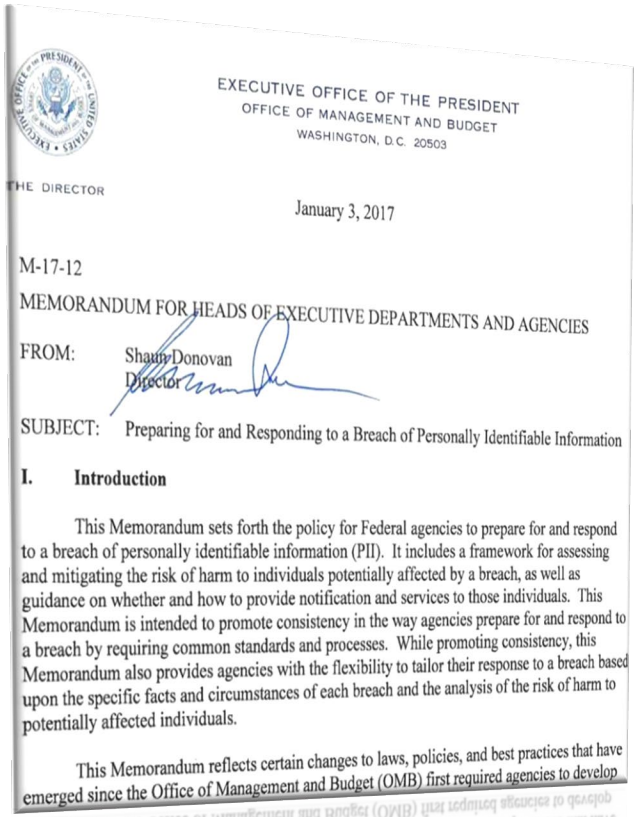
Privacy Incident – is an occurrence (event) that compromises the integrity, confidentiality, or availability of an information asset.

Privacy Breach – is an incident that results in the confirmed disclosure — not just potential exposure — of data to an unauthorized individual.

It's important to note here that the word *incident* is used in the definition of a data breach. This is because while all data breaches are definitely incidents however, not all incidents are data breaches.

OMB – M-17-12

Privacy Incidents: Possible Scenarios



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

January 3, 2017

M-17-12

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shaun Donovan
Director

SUBJECT: Preparing for and Responding to a Breach of Personally Identifiable Information

I. Introduction

This Memorandum sets forth the policy for Federal agencies to prepare for and respond to a breach of personally identifiable information (PII). It includes a framework for assessing and mitigating the risk of harm to individuals potentially affected by a breach, as well as guidance on whether and how to provide notification and services to those individuals. This Memorandum is intended to promote consistency in the way agencies prepare for and respond to a breach by requiring common standards and processes. While promoting consistency, this Memorandum also provides agencies with the flexibility to tailor their response to a breach based upon the specific facts and circumstances of each breach and the analysis of the risk of harm to potentially affected individuals.

This Memorandum reflects certain changes to laws, policies, and best practices that have emerged since the Office of Management and Budget (OMB) first required agencies to develop

According to OMB, "common" examples of a PII breaches are following:

- a laptop or portable storage device storing PII is lost or stolen;
- an email containing PII is inadvertently sent to the wrong person;
- a box of documents with PII is lost or stolen during shipping;
- an unauthorized third party overhears agency employees discussing PII about an individual seeking employment or federal benefits;
- a user with authorized access to PII sells it for personal gain or disseminates it to embarrass an individual;
- an IT system that maintains PII is accessed by a malicious actor, or PII that should not be widely disseminated is posted inadvertently on a public website.

Privacy Incidents: Possible Scenarios (Continue)

SSN is the most frequently lost, stolen or compromised PII data element. SSN is involved in almost 70 percent of breaches.

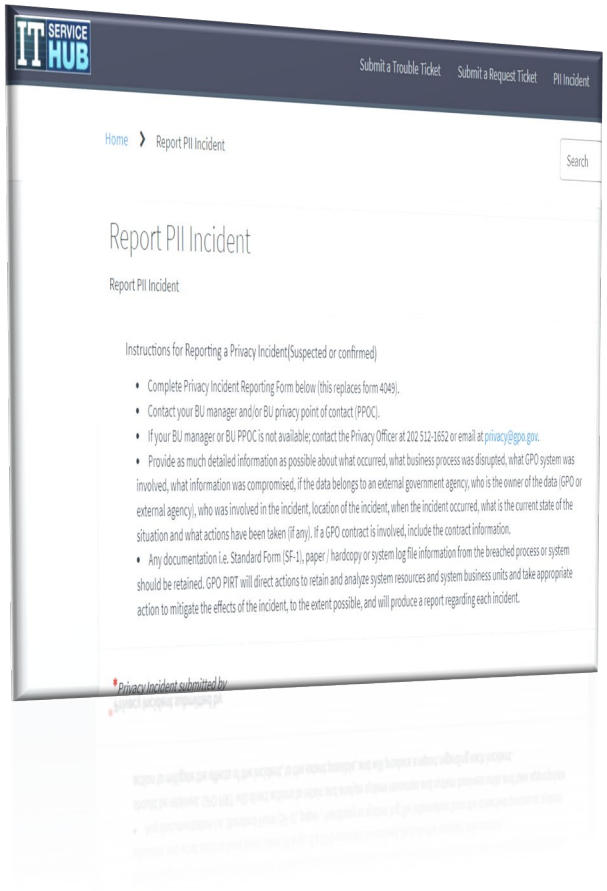
SSN is the sensitive identifier and must be closely safeguarded or eliminated from use.

Human error is the cause of 80 percent of the PII breaches. Not knowing or not following guidance, or just being careless can result in the unintended disclosure of privacy sensitive information and potentially adversely affect many personnel.

Some additional Breach Scenarios

- HR/Payroll/Medical/Education.
- GPO Intranet or public facing website has unredacted PII.
- PII on our servers (GPO/Cloud/Hosted)
- PII in emails being sent/received
- PII on other than electronic media being shipped/received
- Breach of GPO customer provided PII at GPO or Contractor facility, during shipment, electronic transfer, etc.
- Presence of public PII in a GPO website
- Sending SSN in an email or in attachments
- Creating recall rosters with SSNs
- Posting names with associated SSNs to web portals or shared drives

All Privacy Incidents must be reported



The GPO Privacy directive requires, all suspected or actual Privacy (PII) incidents shall be reported using the GPO **Online Privacy Incident Reporting Form,** available at the ITServiceHUB on the GPO Intranet.

The report should be made IMMIDIATELY and include all possible details of the incident; what and when happened, which BU was impacted, what information was compromised (if known), who was involved, what is the current state of the situation, and what actions have already been taken (if any).

Standard Operating Procedure on the Privacy Incident Reporting is available on the GPO Intranet on Information Technology Section.

GPO

How to report Privacy Incidents

GPO Directive 825.41B guides:

#1 Always, immediately notify your supervisor. Also contact your Business Unit manager or Business Unit Privacy Point of Contact (PPOC). List of BU PPOCs is attached.

#2 Access the GPO Online Privacy Incident Reporting Form (OPIRF) available at the GPO Intranet website.

While reporting the Privacy incident, provide as much detailed information as possible about what occurred, when did the incident occur and what information was compromised.

Any paper documentation, webpage URL or system process information from the incident should be reported to GPO.

For more details on how to report a privacy incident, please use Standard Operation Procedure (SOP) “Reporting a Privacy Incident”.

GPO Privacy Incident Response Team (PIRT) will take appropriate action to mitigate the effects of the incident and report its findings as determined by the GPO Privacy Office.

GPO

AI adds another layer of complexity

Photo: N. Hanacek/NIST

Artificial Intelligence (AI) tools and solutions, such as image recognition, speech-to-text, cognitive knowledge, ChatGPT, and many more, may facilitate automated processing, simplifying tasks, and increasing efficiency however, it introduces new challenges.

When collecting sensitive PII data using AI tools or putting PII data into AI tools' database, it may broaden the PII exposure, potentially resulting in additional PII incidents.

AI can also cause another challenge: how to exercise the privacy principle called individual's right to update or remove personal information which with AI becomes more difficult because the data may have crossed the GPO systems' boundaries.

GPO

Risks for not Safeguarding PII

Following deliberate, or unintentional actions are prohibited by the **GPO Directive 825.41B:**

- *removing*
- *concealing*
- *altering*
- *damaging*
- *destroying*
- *deleting*
- *loosing*
- *unapproved sharing*
- *using PII for personal purposes*

The following penalties could potentially apply to an individual who fails to comply with regulations for safeguarding PII:

Employees who fail to protect PII according to established standards and procedures or who disclose PII improperly may be subject to disciplinary action up to and including removal or criminal sanctions and penalties in appropriate cases.

Contractors who fail to protect PII may be subject to termination for default and any other appropriate administrative action.

New employees should fill a “Rules of Behavior Form” (IT Security Form) to acknowledge their awareness of and understanding the importance of safeguarding information, risks associated with any breach, and penalties for not following the specified guidelines.

GPO

Risk For Not Properly Managing Records

There are penalties for unlawfully, deliberately, or accidentally:

- Removing, concealing, or altering Federal records
- Damaging, destroying, deleting, or losing Federal records
- Disclosing national security information
- Using Federal records for personal purposes

The consequences may include one or more of the following:

- A fine, 3 years imprisonment, or both
- Removal from office
- Disqualification from holding any other office in the government.

GPO

Any Questions –
Contact GPO Privacy Program

GPO Privacy Office
Information Technology

U. S. Government Publishing Office
732 North Capitol Street, N.W.
Washington, DC 20401
(202) 512-1652

privacy@gpo.gov