



EFFECTIVE DATE

(03-02-2023)

PURPOSE

- (1) This transmits revised IRM 10.5.4, Privacy and Information Protection, Incident Management Program.

MATERIAL CHANGES

- (1) IRM 10.5.4.1.3, Responsibilities: Deleted the reference to IRM 25.13.1.3 in (3) b) Table as erroneous taxpayer correspondence involving the disclosure of SBU data, including PII and tax information, is no longer being reported to OTC.
- (2) IRM 10.5.4.1.4, Program Management and Review: Reorganized the information contained in (2) a) and added information about the additional data breach categories included on the IRS Quarterly Scorecards.
- (3) IRM 10.5.4.1.8, Related Resources: Inserted new d) listing Document 13347, Data Breach Response Playbook, and new e) listing Document 13347-A, IRS Data Breach Response Plan, in (1). Subsequent paragraphs after new e) renumbered. Inserted new k) listing OMB M-23-07, Update to Transition to Electronic Records, in (2).
- (4) IRM 10.5.4.3.1, Timely Reporting: Immediately Upon Discovery: Added “erroneous taxpayer correspondence involving the disclosure of SBU data, including PII and tax information” to (2) as erroneous taxpayer correspondence involving the disclosure of SBU data, including PII and tax information, is now being reported to PGLD/IM.
- (5) IRM 10.5.4.3.3, Inadvertent Unauthorized Disclosures and Losses or Thefts of IT Assets, BYOD Assets and Hardcopy Records/Documents: Deleted the reference to OTC in (1) as data breaches involving erroneous taxpayer correspondence are no longer being reported to OTC. Added “SAMC” to the text in (1). Deleted (2) a) and the (2) a) Note as erroneous taxpayer correspondence involving the disclosure of SBU data, including PII and tax information, is no longer being reported to OTC. Updated (2) b) (now (2) a) to include erroneous taxpayer correspondence involving the disclosure of SBU data, including PII and tax information; added additional examples of erroneous taxpayer correspondence; re-located some of the Notes; and added a new note with a link to the If/Then Guide for Reporting Incidents and Data Breaches and a reminder to check the TIGTA and Law Enforcement reporting requirements for additional reporting requirements based on what was lost, stolen, destroyed, or disclosed. Reworded (2) c) (now b), and (2) d) (now c), and (3) and (4) for clarity.
- (6) IRM 10.5.4.3.4, Inadvertent Accesses of Tax Information: Deleted the reference to OTC in (3) as inadvertent accesses are not reported to OTC (nor to PGLD/IM or CSIRC).
- (7) IRM 10.5.4.3.5, “No Reporting” Situations: Deleted the reference to OTC and CSIRC in (1) and the Note at the end of the subsection referencing IRM 25.13.1.3 as erroneous taxpayer correspondence involving the disclosure of SBU data, including PII and tax information, is no longer being reported to OTC, and erroneous taxpayer correspondence and unauthorized disclosures aren’t reported to CSIRC. Added a Note after e) to see the No Reporting Situations PDF listed in the Other Related Resources section on the Report Losses, Thefts or Disclosures page in the Disclosure and Privacy Knowledge Base Site.

- (8) IRM 10.5.4.4.1, PGLD/Incident Management Intake: Deleted the reference to OTC in (1) and deleted (1) b) as erroneous taxpayer correspondence involving the disclosure of SBU data, including PII and tax information, is no longer being reported to OTC. Updated (1) a) to include erroneous taxpayer correspondence involving the disclosure of SBU data, including PII and tax information, as it's now being reported to PGLD/IM. Subsequent paragraphs renumbered.
- (9) IRM 10.5.4.4.1, PGLD/Incident Management Intake: Updated (1) c) (now b) to include an additional example of what should be reported to CSIRC.
- (10) IRM 10.5.4.4.4, PGLD/Incident Management Risk Assessment: Added the following to the end of (1): "Note that all data breaches are unique and when making determinations, all facts and circumstances must be considered."
- (11) IRM 10.5.4.4.4, PGLD/Incident Management Risk Assessment: Deleted the words "and action if necessary" at the end of (6) as the Code Red Recommendations Report is sent to the IM Associate Director for review only; no approval is required.
- (12) IRM 10.5.4.4.6.4, Means of Providing Data Breach Notifications: Added "For high-risk data breaches" to the beginning of (3) to clarify that the paragraph is about high-risk data breaches.
- (13) IRM 10.5.4.5.1, IRS Data Breach Tracking Indicator - Development and Implementation: Added "and the data breach risk assessment results in a likelihood of harm to the potentially impacted individuals" to the end of (2) to clarify the criteria for entering the TC 971 AC 505.
- (14) Exhibit 10.5.4-1, Glossary of Incident Management Terms, Definitions, and Acronyms: Added a definition for "Erroneous Taxpayer Correspondence" and "Incorrect Correspondence". Updated the definitions of Form 14164 and Form 14164-A to include erroneous taxpayer correspondence involving the disclosure of SBU data, including PII and tax information, as it's now being reported to PGLD/IM.
- (15) Throughout, made editorial changes to add clarity where necessary; reviewed IRM, document citations, OMB, and legal references and updated them as necessary, including updating OMB M-22-05, Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements, to OMB M-23-03, Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements; reviewed website and webpage links and added or updated them as necessary; corrected capitalization, spelling, typos and grammar as necessary; and incorporated plain language writing techniques. Also ensured URLs for internal links were not included within the text as previously requested by IT/Cyber Policy because of perceived security risks.

EFFECT ON OTHER DOCUMENTS

This IRM supersedes IRM 10.5.4 dated September 2, 2022.

AUDIENCE

The provisions in this manual apply to all IRS personnel in all divisions and functional units. It includes managers, employees, IRS contractors, Volunteer Income Tax Assistance/Tax Counseling for the Elderly volunteers, Flexiplace (Telework) employees (Frequent, Recurring, and Ad Hoc) and Mobile employees.

Peter C. Wade
Director, Privacy Policy and Compliance
Privacy, Governmental Liaison and Disclosure

10.5.4
Incident Management Program

Table of Contents

10.5.4.1 Program Scope and Objectives

- 10.5.4.1.1 Background
- 10.5.4.1.2 Authority
- 10.5.4.1.3 Responsibilities
- 10.5.4.1.4 Program Management and Review
- 10.5.4.1.5 Program Controls
- 10.5.4.1.6 Terms
- 10.5.4.1.7 Acronyms
- 10.5.4.1.8 Related Resources

10.5.4.2 Awareness Training and Education

10.5.4.3 Reporting Losses, Thefts and Disclosures

- 10.5.4.3.1 Timely Reporting: Immediately Upon Discovery
- 10.5.4.3.2 Intentional Unauthorized Disclosures of Tax Information
- 10.5.4.3.3 Inadvertent Unauthorized Disclosures and Losses or Thefts of IT Assets, BYOD Assets and Hardcopy Records/Documents
- 10.5.4.3.4 Inadvertent Accesses of Tax Information
- 10.5.4.3.5 “No Reporting” Situations

10.5.4.4 PGLD/Incident Management Intake, Risk Assessment and Notification

- 10.5.4.4.1 PGLD/Incident Management Intake
- 10.5.4.4.2 High-Risk Data Breaches
- 10.5.4.4.3 OMB Major Incidents
- 10.5.4.4.4 PGLD/Incident Management Risk Assessment
- 10.5.4.4.5 The PII Working Group (PIIWG)
- 10.5.4.4.6 PGLD/Incident Management Data Breach Notification - Letter 4281C
 - 10.5.4.4.6.1 Contents of the Data Breach Notification Letter
 - 10.5.4.4.6.2 Data Breach Notification Signature
 - 10.5.4.4.6.3 Timeliness of the Data Breach Notification
 - 10.5.4.4.6.4 Means of Providing Data Breach Notifications
- 10.5.4.4.7 Ongoing Support
 - 10.5.4.4.7.1 Handling Inquiries About IM Data Breach Notification Letters
 - 10.5.4.4.7.2 IMF Identity Check - AM IDT Toll-Free (App 161/162) Telephone Overview
 - 10.5.4.4.7.3 BMF Identity Check - AM IDT Toll-Free (App 161/162) Telephone Overview
 - 10.5.4.4.7.4 Free Identity Protection/Identity Monitoring Service
 - 10.5.4.4.7.5 Fraud Alerts
 - 10.5.4.4.7.6 Referrals to PGLD’s Incident Management Office

- 10.5.4.4.7.7 Caller Indicates He or She is a Victim of Identity Theft as a Result of an IRS Data Breach
- 10.5.4.4.7.8 Updating History on Accounts Management Services (AMS) for Calls About IRS Data Breach Notification Letters
- 10.5.4.4.7.9 Undelivered Letter 4281C
- 10.5.4.4.8 Retention and Disposition
- 10.5.4.5 IRS Data Breach Tracking Indicator - Objectives
 - 10.5.4.5.1 IRS Data Breach Tracking Indicator - Development and Implementation
 - 10.5.4.5.1.1 Applying the IRS Data Breach Tracking Indicator to IRS Data Breaches

Exhibits

- 10.5.4-1 Glossary of Incident Management Terms, Definitions, and Acronyms
- 10.5.4-2 TC 971 AC 505 — IRS Data Breach Indicator
- 10.5.4-3 TC 972 AC 505 — Reversal of TC 971 AC 505

10.5.4.1
(09-02-2022)
**Program Scope and
Objectives**

- (1) **Purpose.** This IRM provides procedural guidance for reporting IRS data losses, thefts, and inadvertent unauthorized disclosures involving Sensitive But Unclassified (SBU) data, including Personally Identifiable Information (PII) and tax information.
- (2) **Audience.** The provisions in this manual apply Servicewide whenever SBU data, including PII and tax information, is collected, created, transmitted, used, processed, stored, or disposed of, in support of the IRS mission. This manual also applies to individuals and organizations having contractual arrangements with the IRS, including contractors, subcontractors, vendors, Volunteer Income Tax Assistance/Tax Counseling for the Elderly volunteers, and any other outsourced providers doing business with the IRS. This manual also applies to all Flexiplace (Telework) employees (Frequent, Recurring and Ad Hoc) as well as Mobile employees.
 - a. All IRS employees, contractors/vendors, and persons with authorized access to SBU data, including PII and tax information, are responsible and accountable for complying with federal and IRS privacy, information protection, and data security, policies and procedures. Safeguarding and preventing the unauthorized disclosure of SBU data, including PII and tax information, is a responsibility that is shared by *all IRS employees, contractors/vendors, and persons with authorized access to SBU data, including PII and tax information*. Lost, stolen, or disclosed SBU data, including PII and tax information, may be used to perpetrate identity theft or other forms of harm, if the information falls into unauthorized hands. See IRM 10.5.4.4.4, *PGLD/Incident Management Risk Assessment*, and Exhibit 10.5.4-1, *Glossary of Incident Management Terms, Definitions, and Acronyms*, for additional information about, and examples of, **harm/risk of harm**.
 - b. All tax, privacy, and security clauses must be included in contracts as required by IRM 11.3.24, *Disclosure of Official Information, Disclosures to Contractors*, and IRM 10.5.6.2, *Privacy Act General Provisions (formerly IRM 11.3.14)*. Contractor employees must be trained about SBU data protection requirements, including PII and tax information, as required in Treasury Regulation 301.6103(n)-1(d).
 - c. IRS Acquisition Policy (IRSAP) Part 1004, Administrative Matters, and IRSAP Part 1024, Protection of Privacy and Freedom of Information, provide instructions with respect to procedures to be followed where contractual procurement will be subject to the Privacy Act, the provisions of IRC 6103(n), or where access by a contractor to Sensitive But Unclassified material is contemplated.
 - d. For additional information about security controls, see IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance*, and Pub 4812, *Contractor Security and Privacy Controls*.
- (3) **Policy Owner.** The Privacy Policy and Compliance (PPC) Director is responsible for the policy in this IRM. PPC is under the Office of Privacy, Governmental Liaison and Disclosure (PGLD), which is under the Office of the Deputy Commissioner for Operations Support (OS).
- (4) **Program Owner.** The Incident Management Office under the Office of Privacy Policy and Compliance (PPC) under PGLD is the program office responsible for this IRM.

- (5) **Primary Stakeholders.** All employees and contractors of the IRS, in all divisions and functional units, including Flexiplace (Telework) employees (Frequent, Recurring and Ad Hoc) and Mobile employees, are affected by the procedures in this IRM.
- (6) **Contact Information.** To recommend changes to this IRM section, email the **PII mailbox*.

10.5.4.1.1
(09-02-2022)
Background

- (1) **Overview.** This IRM defines the mission, objectives, and governance structure of the Privacy Policy and Compliance Incident Management Program. It provides the organizational framework for carrying out specific policies and procedures aimed at timely reaction and appropriate responses to occurrences of IRS data losses, thefts, and inadvertent unauthorized disclosures involving SBU data, including PII and tax information.
- (2) **Privacy, Governmental Liaison and Disclosure (PGLD).** Privacy, Governmental Liaison and Disclosure (PGLD), previously known as *Privacy, Information Protection and Data Security (PIPDS)*, is responsible for ensuring consistency in all processes and procedures affecting the ways the IRS handles privacy information protected by statute, regulation, Executive Order, or internal policy.
 - a. PGLD works with other Business Units to provide the IRS with the tools and resources necessary to protect sensitive taxpayer and employee data from potential identity theft due to IRS incidents involving the loss or theft of IRS IT assets and Bring Your Own Device (BYOD) assets containing SBU data, including PII and tax information; the loss or theft of physical and electronic documents that include SBU data, including PII and tax information; and inadvertent unauthorized disclosures of SBU data, including PII and tax information.
 - b. PGLD also leads IRS privacy and records policies, coordinates privacy protection guidance and activities, responds to privacy complaints, and promotes data protection awareness throughout the IRS.
- (3) **PGLD Incident Management (IM) Office.** IM was established to ensure Servicewide implementation of federal directives to protect taxpayers and government employees against IRS data losses and misuse of sensitive personal data.
 - a. Since September 2007, the IM Office (previously known as the ITIM Office) in PGLD (previously known as PIPDS) has been responsible for administering and managing IRS program requirements by ensuring IRS incidents involving the loss or theft of IRS IT assets and BYOD assets containing SBU data, including PII and tax information; the loss or theft of physical and electronic documents that include SBU data, including PII and tax information; and inadvertent unauthorized disclosures of SBU data, including PII and tax information, are investigated, analyzed and resolved by PGLD/IM.
 - b. IM is dedicated to assisting taxpayers and government employees potentially impacted by IRS incidents involving SBU data, including PII and tax information, by working quickly and thoroughly to investigate the incidents to decrease the possibility that the information will be compromised and used to perpetrate identity theft or other forms of harm. See IRM 10.5.4.4.4, *PGLD/Incident Management Risk Assessment*, and Exhibit 10.5.4-1, *Glossary of Incident Management Terms, Definitions, and*

Acronyms, for additional information about, and examples of, **harm/risk of harm**.

- c. IM manages the reporting, risk assessment, and tracking of IRS incidents involving SBU data, including PII and tax information, as well as notification to potentially impacted individuals.

Note: IM *isn't* responsible for any disciplinary actions that can result from an employee's or manager's failure to protect IT equipment or information, employee data, SBU data, or PII, nor is IM responsible for contacting Labor Relations regarding a manager's or employee's failure to protect IT equipment or information, employee data, SBU data, or PII.

10.5.4.1.2
(09-02-2022)
Authority

- (1) Federal agencies have been instructed by the Office of Management and Budget (OMB) and the Department of the Treasury to address the increasing occurrence of identity theft and to safeguard Personally Identifiable Information (PII).
- (2) Executive Order 13402, May 10, 2006, established the President's Identity Theft Task Force. The Task Force recommended that Federal agencies reduce the incidence and impact of identity theft and improve their capacity to respond to data breaches. The Task Force recognized that any comprehensive information security program - whether in the public or private sector - must include policies for responding to a data breach. Although every breach is different, experience has shown that having policies in place in advance is critical to ensuring a proper response. Such policies should address whether, how, and when to inform potentially impacted individuals of the loss of their data, and whether to offer services such as free credit monitoring to those individuals. The Task Force developed guidance that OMB issued to all agencies and departments on September 20, 2006, on responding to data breaches that pose a risk of identity theft. The guidance provided agencies with a framework for conducting an analysis of the breach to determine whether the breach posed a significant risk of identity theft and offered practical advice on implementing a breach response plan, including how and when to provide notice to potentially impacted individuals. To further the goals of the Task Force guidance, in May 2007, OMB issued Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, which emphasized agencies' responsibilities under existing laws, such as the Privacy Act of 1974, to safeguard PII, and instructed Federal agencies to enhance their safeguards for PII and to enact data breach handling and data breach notification policies. The President's Identity Theft Task Force Report of September 2008, <https://www.ftc.gov/sites/default/files/documents/reports/presidents-identity-theft-task-force-report/081021taskforcereport.pdf>, documented the Task Force's efforts to implement the Strategic Plan's recommendations.
- (3) In January 2017, OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2017/m-17-12_0.pdf, rescinded and replaced OMB Memorandum M-07-16, updated *existing* OMB data breach notification policies and guidelines in accordance with the Federal Information Security Modernization Act of 2014 (FISMA), and implemented recommendations included in OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*.

- (4) See IRM 10.5.4.1.8, *Related Resources*, for a list of other relevant OMB Memoranda, Federal Guidance, and IRMs, and details about where to locate them.
- (5) The Incident Management Program was created in response to OMB directives and the President's Identity Theft Task Force recommendations, and to ensure IRS compliance with OMB requirements for data breach management and data breach notification. Consistent with the OMB directives, the IRS notifies potentially impacted individuals when the data breach risk assessment results in a likelihood of harm to the potentially impacted individuals. See IRM 10.5.4.4.4, *PGLD/Incident Management Risk Assessment*, and Exhibit 10.5.4-1, *Glossary of Incident Management Terms, Definitions, and Acronyms*, for additional information about, and examples of, **harm/risk of harm**.

10.5.4.1.3
(03-02-2023)
Responsibilities

- (1) **Incident Management Program Oversight.** The Privacy Policy and Compliance (PPC) Director is the executive responsible for oversight of this program. PPC is under the Office of Privacy, Governmental Liaison and Disclosure (PGLD), which is under the Office of the Deputy Commissioner for Operations Support (OS). The Incident Management and Employee Protection (IMEP) Associate Director reports to the PPC Director, and oversees the IMEP program.
- (2) **Incident Management Program.** The Incident Management Program includes the management of the IRS data breach reporting process, as well as the risk assessment and tracking of IRS data breaches and notification to individuals potentially impacted by IRS data breaches. The Incident Management Program also includes output from Cybersecurity's *Safeguarding Personally Identifiable Information Data Extracts* (SPIIDE) application. IM receives events for investigation, addresses applicable receipts within established procedures, and collaborates on referred events not meeting IM's criterion.
 - a. IM has the following responsibilities related to administering the Incident Management Program in the IRS:
 - Interpreting federal laws, regulations, and policies relating to the protection of Personally Identifiable Information (PII). See IRM 11.3.1, *Disclosure of Official Information, Introduction to Disclosure*, for more information about the Disclosure program and the protection of official information including personal information and tax records.
 - Coordinating with other program areas in the IRS to ensure compliance with OMB Memorandum M-17-12 and related directives
 - Receiving SPIIDE events for investigation and addressing accordingly when received
 - Conducting risk assessments of IRS data breaches and determining how to best mitigate the identified risks, such as providing identity protection/identity monitoring services, or offering guidance on how the potentially impacted individuals can mitigate their own risk of harm, such as setting up fraud alerts or credit freezes, changing or closing accounts, etc.
 - Analyzing and tracking IRS data breaches reported to the IM office as well as contacting the BU data owner or Reporting Employee for additional information concerning the incident or data breach
 - Notifying potentially impacted individuals (if the data breach risk assessment results in a likelihood of harm, such as the potential for identity theft)

- Reporting weekly to the Records and Information Management (RIM) Program Office any incidents of lost, stolen, or destroyed records
- Identifying risks associated with IRS data breaches and collaborating with the BU data owner on mitigating the risks
- Preparing all reporting documentation pertaining to IRS data breaches
- Making notification recommendations about potentially impacted individuals based on assessed risk and consulting with appropriate law enforcement officials and other offices or authorities if necessary
- Identifying emerging trends and developing appropriate strategies and responses
- Improving procedures to reduce the occurrence of IRS incidents and data breaches
- Developing, defining, monitoring, and executing IM policies and procedures
- Overseeing the maintenance, publication, and conveyance of the Privacy and Information Protection Incident Management IRM
- Communicating and coordinating with internal stakeholders to ensure consistency about data breach policy and issues

Note: IM *isn't* responsible for any disciplinary actions that can result from an employee's or manager's failure to protect IT equipment or information, employee data, SBU data, or PII, nor is IM responsible for contacting Labor Relations regarding a manager's or employee's failure to protect IT equipment or information, employee data, SBU data, or PII.

(3) **Reporting Employees and Business Unit (BU) Data Owners.** In addition to timely reporting (immediately upon discovery) so PGLD/IM can begin its risk assessment process, reporting employees and/or BU data owners have other responsibilities such as containment, mitigation, prevention, providing information requested by PGLD/IM within two business days of request, taking disciplinary actions, and contacting potentially impacted individuals to request replacement documents. See a) thru f) below for a description of the reporting employee and/or BU data owner responsibilities. Also see IRM 10.5.4.3.1, *Timely Reporting: Immediately Upon Discovery*, for additional information about **timely reporting**.

- a. **Containment.** The BU data owner must take immediate action to contain the incident or data breach to prevent any further PII exposure, e.g., if employee or taxpayer data is inadvertently exposed on the internet, the BU data owner must immediately take steps to remove the data and/or close the access; or, if DVDs have been shared with material that should have been redacted, the BU must take steps to immediately recover them and request the recipient remove public access (if the information was made publicly available) and replace it with the proper data. The BU should contact Cybersecurity's Online Fraud Detection and Prevention Office if assistance is required to contain a data breach involving an electronic transmission such as email or a data breach involving the posting of information on the internet. Additional actions related to containment will depend on the nature of the breach and may involve other BUs as needed.

Note: If the employee reporting the data breach is not the BU data owner, the reporting employee must collaborate with the BU and PGLD/IM to determine the best approach for managing containment.

Note: The BU data owner will ensure PGLD/IM is apprised of any containment actions taken. PGLD/IM will document the containment actions taken by the BU on e-Trak.

- b. **Mitigation.** The BU data owner must analyze the event circumstances to mitigate or lessen the impact of the incident or data breach. Necessary actions may include requesting the person who erroneously received a notice, letter, or transcript, to return or destroy it; asking the incorrect recipient of a fax, EEFax, email, etc., to destroy or delete it; or asking the person who received an erroneously addressed or misdelivered shipment to secure the shipment and await collection by an IRS employee. Necessary actions by the BU may also include physically recovering hardcopy documents or coordinating with TIGTA to ensure all recovery options are considered.

If	Then
If a notice, letter, or transcript is sent in error to the wrong person and not the last known address of record, or multiple correspondence for different taxpayers are included in one envelope	The BU data owner must ask the person who incorrectly received the notice, letter, or transcript to return the document, or, if the person refuses to return the document, ask them to destroy it.
If a fax, EEFax, email, or other electronic transmission is sent to the wrong addressee	The BU data owner must ask the person who incorrectly received the fax, EEFax, email, or other electronic transmission, to delete it or destroy it (if printed).
If a shipment is erroneously addressed or misdelivered, and the recipient contacts the IRS regarding the erroneously received shipment	The BU data owner must take steps to recover the shipment.

Note: The BU data owner must ensure PGLD/IM is apprised of any mitigation actions taken. PGLD/IM will document the mitigation actions taken by the BU on e-Trak.

- c. **Prevention.** The BU data owner must determine the necessary steps to prevent similar incidents or data breaches in the future. This could entail investigating the cause of the incident or data breach and developing a prevention plan if necessary. A prevention plan may include a security audit of both physical and technical security, a review and/or development of policies and procedures, and a review of employee training.

Note: The BU data owner must ensure PGLD/IM is apprised of any prevention actions taken. PGLD/IM will document the prevention actions taken by the BU on e-Trak.

- d. **Providing Requested Information.** The reporting employee or BU data owner must provide all information requested by PGLD/IM, e.g., complete, unredacted SSNs, names, dates, etc., **within two business days of request to ensure timely reporting and taxpayer notification.** If a delay is likely, contact IM at 267-466-0777 to facilitate next steps.

Note: If the unredacted (not truncated) SSNs for the potentially impacted individuals involved in the data breach are not readily available, **the Reporting Employee or BU data owner must research to determine the complete SSNs.** After due diligence, if the unredacted SSNs for the potentially impacted individuals cannot be determined, email the *PII mailbox, or contact IM at 267-466-0777.

- e. **Disciplinary Actions.** Discipline can result for failure to protect equipment or information, as well as for a manager's failure to supervise and train as it pertains to PII information. A BU data owner whose employee experiences a data loss, theft, or disclosure, or asset loss or theft, because the employee did not properly safeguard the data or asset, must contact the servicing Labor Relations Specialist to discuss the appropriateness of any disciplinary action. For disciplinary actions related to losses or thefts of laptops or other electronic devices, or the loss, theft or disclosure of SBU data, including PII and tax information, and improperly safeguarding electronic or paper records, see Document 11500, *IRS Manager's Guide to Penalty Determinations*, and IRM 6.751.1, *Discipline and Disciplinary Actions: Policies, Responsibilities, Authorities, and Guidance*.

Note: PGLD/IM *isn't* responsible for any disciplinary actions that can result from an employee's or manager's failure to protect IT equipment or information, employee data, SBU data, or PII, nor is IM responsible for contacting Labor Relations regarding a manager's or employee's failure to protect IT equipment or information, employee data, SBU data, or PII.

- f. **Contacting Potentially Impacted Individuals to Request Replacement Documents.** Although PGLD/IM notifies the potentially impacted individuals of an IRS data breach if it's determined there's a potential risk of harm to the individuals as a result of the data breach (such as the potential for identity theft), the BU data owner is responsible for contacting the potentially impacted individuals if an original document, or remittance (such as a personal check), was lost, stolen, or destroyed, to explain that the original document or remittance was lost, stolen, or destroyed, and to request that the individual resend the document or remittance. Established functional taxpayer contact processes must be followed when requesting replacement documents or remittances from the potentially impacted individuals. See IRM 10.5.4.4.4, *PGLD/Incident Management Risk Assessment*, and Exhibit 10.5.4-1, *Glossary of Incident Management Terms, Definitions, and Acronyms*, for additional information about, and examples of, **harm/risk of harm**.

Note: In addition to requesting replacement documents or remittances, contact with the potentially impacted individuals may include a brief, general explanation of the data breach, e.g., "a package containing your document (or remittance) was lost in shipment." If the **BU data owner** has any questions about contacting the potentially impacted individuals about the data breach, the BU data owner may call PGLD/IM at 267-466-0777 or email the *PII mailbox. **Do not share the telephone number or mailbox address with the potentially impacted individuals.**

- (4) In the event you or your Business Unit is called upon to participate as part of a Breach Response Team (BRT), there are specific activities you may be required to conduct based on your specific Business Unit and/or role in the

organization. See the *High-Risk Data Breach Quick Reference Guide* listed in the **Other Related Resources** section of the *Report Losses, Thefts or Disclosures* page in the *Disclosure and Privacy Knowledge Base Site* and Document 13347, *Data Breach Response Playbook*, for additional information on the activities you may be required to conduct. Also see IRM 10.5.4.4.2, *High-Risk Data Breaches*, for additional information concerning high-risk data breaches.

- (5) For the definition of *Reporting Employee* and *Business Unit (BU) Data Owner*, see IRM 10.5.4.1.6, *Terms*, and Exhibit 10.5.4-1, *Glossary of Incident Management Terms, Definitions, and Acronyms*.

10.5.4.1.4
(03-02-2023)
**Program Management
and Review**

- (1) PGLD/IM has established Business and Organizational measures to measure the timeliness of IRS data breach notifications to potentially impacted individuals of IRS data breaches. See IRM 10.5.4.4.6.3, *Timeliness of the Data Breach Notification*.
- (2) PGLD/IM provides reports on Business Performance as it relates to IRS data breaches to Points of Contact within each Business Unit. The reports can be used by PGLD/IM as well as the BUs to identify trends as well as training and outreach opportunities.
- a. **Quarterly Scorecard Report.** The Quarterly Scorecard Reports (in PDF format) list the number of reported data breaches received by PGLD/IM per quarter per Business Operating Division (BOD). The Reports, which are shared with each respective BOD, provide an analysis of all reported data breaches identified as a loss, theft, or inadvertent unauthorized disclosure based on the type of asset, location, and risk assessment code. The Quarterly Scorecard Report is also shared with the Privacy Compliance office in PGLD to determine if there are any processes for which a Business PII Risk Assessment (BPRA) can be performed. The BPRA is used to identify vulnerabilities and make recommendations for changes to improve IRS security and privacy policies and practices. A separate Quarterly Scorecard Report capturing the performance of the IRS overall is also provided to each BOD. The IRS Quarterly Scorecard Report provides an analysis of all reported data breaches identified as a loss, theft, or inadvertent unauthorized disclosure as well as those identified as **other**, such as Private Debt, SPIIDE, UNAX, etc.
 - b. **Quarterly E-Trak Data Extract Report.** The e-Trak Data Extract Reports (in Excel format), which list the losses, thefts, and inadvertent unauthorized disclosures reported to PGLD/IM per BOD, is usually provided quarterly but can be provided more frequently (such as monthly) upon request by the BOD. The extract provides an analysis of all reported data breaches identified as a loss, theft, or inadvertent unauthorized disclosure based on the type of asset, location, reporting employee, and risk assessment code.
 - c. **Weekly Code Red Recommendations Reports.** The Code Red Recommendations Report lists data breaches potentially impacting individuals likely to be at risk of identity theft or other harm due to the loss, theft, or disclosure of PII. The Report is presented to the PII Working Group weekly by PGLD/IM for information only; no concurrence or approval by the PII Working Group (PIIWG) is required.

10.5.4.1.5
(09-02-2022)
Program Controls

- (1) Program controls developed to oversee the Incident Management Program include the following:
 - a. PGLD/IM conducts quarterly Operational Reviews to evaluate key performance measures to ensure agency program requirements are met.
 - b. PGLD/IM uses established Business and Organizational measures to measure the timeliness of IRS data breach notifications.
 - c. PGLD/IM uses the Quarterly Scorecard Report which contains information from e-Trak (a web interface for case tracking) to assess Business Unit and IRS performance.
 - d. PGLD/IM reconciles redeemed identity protection/identity monitoring codes monthly to ensure the codes assigned to potentially impacted individuals via Letter 4281C were redeemed by the individuals to whom they were assigned before the monthly invoice is paid.
 - e. PGLD/IM generates a Code Red Recommendations Report weekly listing the data breaches deemed to be Code Red (data breaches requiring notifications) to notify the PPC Director and the IMEP Associate Director of the data breaches pending notification.
 - f. PGLD/IM reviews all PII Breach Reporting Forms and alerts the Records and Information Management (RIM) Program Office if official records have been reported as lost, stolen, or destroyed on the PII Breach Reporting Form in accordance with IRM 1.15.3.4, *Unauthorized Disposition of Records*, and 36 CFR 1230, *Unlawful or Accidental Removal, Defacing, Alteration, or Destruction of Records*.

10.5.4.1.6
(09-02-2022)
Terms

- (1) **Incident.** OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2017/m-17-12_0.pdf, defines an incident as an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
 - a. An incident involving the loss or theft of an IRS IT asset or BYOD asset containing PII, or the loss or theft of a physical document that includes PII, or the inadvertent unauthorized disclosure of PII, is known as a data breach. See the **Data Breach** definition below. Often, an occurrence may be first identified as an incident, but later identified as a data breach once it is determined that the incident involves PII, as is often the case with a lost or stolen laptop or electronic storage device.
- (2) **Data Breach.** A data breach is a type of incident involving a loss, theft, or inadvertent unauthorized disclosure of PII. OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2017/m-17-12_0.pdf, defines a data breach as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or, (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose.
 - a. A data breach is not limited to an occurrence where a person other than an authorized user potentially accesses PII by means of a network intru-

sion, a targeted attack that exploits website vulnerabilities, or an attack executed through an email message or attachment. A data breach may also include the loss or theft of physical documents that include PII and portable electronic storage media that store PII, the inadvertent disclosure of PII on a public website, or an oral disclosure of PII to a person who is not authorized to receive that information. It may also include an authorized user accessing PII for an other than authorized purpose. Often, an occurrence may first be identified as an incident, but later identified as a data breach once it's determined that the incident involves PII, as is often the case with a lost or stolen laptop or electronic storage device.

- b. Some common examples of a data breach include:
- A laptop or electronic storage media containing PII is lost or stolen.
 - A document containing PII is lost or stolen, or lost or stolen during shipping.
 - A verbal disclosure of PII to an individual not authorized to receive it.
 - An email containing PII is sent to the wrong person or not properly encrypted.
 - An IT system that maintains PII is accessed by a malicious actor.
 - An inadvertent disclosure of PII on a public website.
 - An authorized user accesses PII for other than an authorized purpose.

(3) **Major Incident.** OMB Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*, <https://www.whitehouse.gov/wp-content/uploads/2022/12/M-23-03-FY23-FISMA-Guidance-2.pdf>, defines a “major incident” as:

- a. Any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people; or,
- b. A breach that involves personally identifiable information (PII) that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people.

Note: OMB-M-23-03 requires a determination of major incident for any unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to the PII of 100,000 or more individuals.

- (4) **Potentially Impacted Individual.** Individuals, as defined by the Privacy Act of 1974, potentially impacted by occurrences of IRS data losses, thefts, and inadvertent unauthorized disclosures involving Sensitive But Unclassified (SBU) data, including Personally Identifiable Information (PII) and tax information, are known as “Potentially Impacted Individuals.” Consistent with OMB directives, the IRS notifies potentially impacted individuals when a data breach involves the loss, theft, or inadvertent unauthorized disclosure of PII, and the result of the risk assessment indicates there is a potential risk that the compromised data may be used by someone other than the owner of the information to commit a crime or fraud.
- (5) **Records Loss.** “Records loss” is defined as the theft or unauthorized destruction, deletion, or removal of any record (or device containing records) under an employee’s control, which cannot be recreated or restored.

- a. **Records.** The term “records” includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them. (44 USC 3301).
 - b. **Unauthorized Destruction.** Unauthorized destruction is the removal from the legal custody of the Federal Government or the alienation, alteration, or mutilation of records without regard to the provisions of IRS Records Control Schedules (RCS 8 through 37) located in IRS Document 12990, *Records and Information Management Records Control Schedules* (Catalog 57910D), and General Records Schedules (GRS) located in IRS Document 12829, *General Records Schedules* (Catalog 54713E).
 - c. **Reporting to NARA.** Per 36 CFR 1230.14, **How do agencies report incidents?**, all federal agencies must report promptly any unlawful or accidental removal, defacing, alteration, or destruction of records in the custody of that agency to the National Archives and Records Administration (NARA). The IRS Records Officer reports any IRS incidents of erroneous records destruction to NARA.
- (6) **Personally Identifiable Information (PII).** The definition of personally identifiable information is provided by OMB in OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2017/m-17-12_0.pdf.
- a. The term PII refers to information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual.
 - b. Some examples of PII are: name, such as full name, maiden name, mother’s maiden name, alias, or name control (first four letters of last name); address information, such as street address or email address; a unique set of numbers or characters assigned to a specific individual, such as telephone numbers, Social Security number (or last four digits of SSN), passport number, driver’s license number, email or Internet Protocol (IP) address, or Standard Employee Identifier (SEID); personal characteristics and data, such as date and place of birth, age, height, or weight; and biometric information such as x-rays, fingerprints, retina scan, or DNA.
 - c. For more information about PII and additional examples, visit the *Personally Identifiable Information* page in the *Disclosure and Privacy Knowledge Base Site*; see IRM 10.5.1, *Privacy and Information Protection, Privacy Policy*; and IRM 10.8.1.3.16.1.3, *Personally Identifiable Information (PII)*.
- (7) **Sensitive But Unclassified (SBU) Data.** Any information which if lost, stolen, misused, or accessed or altered without proper authorization, may adversely affect the national interest or the conduct of federal programs (including IRS operations), or the privacy to which individuals are entitled under the Privacy Act.
- a. SBU data includes, but is not limited to: Federal Tax Information (FTI), Personally Identifiable Information (PII), Protected Health Information

(PHI), certain procurement information, system vulnerabilities, case selection methodologies, systems information, enforcement procedures, and investigation information.

- b. SBU data includes categories of protected information which many IRS personnel handle on a daily basis, such as PII and tax information. It also includes other categories, such as procurement (which can include general procurement and acquisition, small business research and technology, and source selection) and system information (which can include critical infrastructure categories like information systems vulnerability information, physical security, and emergency management).
- c. For more information about SBU, visit the *Sensitive But Unclassified (SBU) Data* page in the *Disclosure and Privacy Knowledge Base Site* and IRM 10.5.1, *Privacy and Information Protection, Privacy Policy*.

(8) **Tax Information.** The term tax information refers to a taxpayer's return and return information protected from unauthorized disclosure under IRC 6103, **Confidentiality And Disclosure of Returns and Return Information.** The law defines return information as any information the IRS has about a tax return or liability determination. See IRC 6103(b)(2) which defines the term **return information.**

- a. Return information includes, but is not limited to, a taxpayer's: identity; income, payments, deductions, exemptions, or credits; assets, liabilities, or net worth; and tax liability investigation status (whether the IRS ever investigates or examines the return).
- b. Redacting, masking, truncating, or sanitizing tax information does not change its nature. It's still tax information.
- c. Tax information in IRS business processes comes under many names, such as FTI, IRC 6103 protected information, taxpayer data, taxpayer information, tax return information, return information, case information, SBU data, and PII.
- d. Tax information is SBU data. IRC 6103 protects tax information from unauthorized disclosure. When tax information relates to an individual, that SBU data is also PII.
- e. Release of tax information (whether of an individual or business) is restricted by the confidentiality provisions of IRC 6103(a).
- f. For more information about tax information, see IRM 10.5.1, *Privacy and Information Protection, Privacy Policy*.

Note: Generally, any response provided by the IRS about a tax return is protected information. Confirming the existence of a tax return (whether a return was or was not filed), or confirming the SSN or EIN of a taxpayer, is prohibited - even a Yes/No response is protected information unless the disclosure is authorized by IRC 6103 and the recipient is authorized to receive it.

(9) **Safeguarding Personally Identifiable Information Data Extracts (SPIIDE) Automated Data Loss Prevention (DLP) Tool.** SPIIDE is a Data Loss Prevention (DLP) tool within the IRS Cybersecurity toolkit.

(10) **Business Unit (BU) Data Owner.** The BU data owner is the Business Unit who has responsibility for the information and is therefore responsible for containment and mitigation of the data breach, e.g., if a Power of Attorney (POA) tells an SBSE Revenue Officer (RO) she received Income Verification Express Service (IVES) transcripts she did not request, the reporting employee is the RO, but W&I is the data owner and carries the responsibility for mitigation and containment.

- (11) **Reporting Employee.** The reporting employee is the employee who identifies/ recognizes a data breach and reports the data breach as required. The reporting employee is responsible for reporting all pertinent information relative to the data breach.
- (12) For a full listing of IM terms and their definitions, see Exhibit 10.5.4-1, *Glossary of Incident Management Terms, Definitions, and Acronyms*.

10.5.4.1.7
(09-02-2022)
Acronyms

- (1) The table below lists commonly used acronyms and their definitions:

Acronym	Definition
BRT	Breach Response Team
BU	Business Unit
BYOD	Bring Your Own Device
CSIRC	Computer Security Incident Response Center
FTI	Federal Tax Information
IM	Incident Management
IMEP	Incident Management and Employee Protection
OMB	Office of Management and Budget
OTC	Office of Taxpayer Correspondence
PGLD	Privacy, Governmental Liaison and Disclosure
PII	Personally Identifiable Information
PIIWG	PII Working Group
PIPDS	Privacy, Information Protection and Data Security (name changed to Privacy, Governmental Liaison and Disclosure (PGLD))
PPC	Privacy Policy and Compliance
RIM	Records and Information Management
SAMC	Situational Awareness Management Center
SPIIDE	Safeguarding Personally Identifiable Information Data Extracts
SBU	Sensitive But Unclassified

- (2) For a full listing of IM terms, definitions, and acronyms, see Exhibit 10.5.4-1, *Glossary of Incident Management Terms, Definitions, and Acronyms*.

10.5.4.1.8
(03-02-2023)
Related Resources

- (1) For additional information and guidance concerning incident/data breach reporting, see the following **internal** resources (for IRS use only):
 - a. The *Disclosure and Privacy Knowledge Base Site*
 - b. The *Report Losses, Thefts or Disclosures* page in the Disclosure and Privacy Knowledge Base Site

- c. The **If/Then Guide for Reporting Incidents and Data Breaches** which is listed in the **Other Related Resources** section of the *Report Losses, Thefts or Disclosures* page in the Disclosure and Privacy Knowledge Base Site
 - d. Document 13347, Data Breach Response Playbook
 - e. Document 13347-A, IRS Data Breach Response Plan
 - f. Document 13056, *Shipping Procedures for Personally Identifiable Information (PII)*
 - g. Document 13144, *Proper PII Shipping Procedures*
- (2) **OMB Memoranda.** OMB Memoranda are available on the *Office of Management and Budget* page at <https://www.whitehouse.gov/omb/information-for-agencies/memoranda/>.
- a. M-06-15, *Safeguarding Personally Identifiable Information*, May 22, 2006. This Memorandum was rescinded and replaced by OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*.
 - b. M-06-16, *Protection of Sensitive Agency Information*, June 23, 2006. This Memorandum was rescinded by OMB Memorandum M-17-15, *Rescission of Memoranda Relating to Identity Management*.
 - c. M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 12, 2006. This Memorandum was rescinded and replaced by OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*.
 - d. M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007. This Memorandum was rescinded and replaced by OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*.
 - e. M-12-18, *Managing Government Records Directive*, November 28, 2011. This Memorandum was rescinded by OMB Memorandum M-19-21, *Transition to Electronic Records*.
 - f. M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, October 30, 2015. This Memorandum was rescinded by OMB Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program*.
 - g. M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 3, 2017. This Memorandum rescinded and replaced OMB Memoranda M-07-16, M-06-19, M-06-15, and *Recommendations for Identity Theft Related Data Breach Notification* (September 20, 2006).
 - h. M-19-03, *Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program*, December 10, 2018. This Memorandum consolidated and updated previous requirements from OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, and OMB Memorandum M-17-09, *Management of Federal High Value Assets*.
 - i. M-19-21, *Transition to Electronic Records*, June 28, 2019. This memorandum rescinded OMB Memorandum M-12-18, *Managing Government Records Directive*.
 - j. M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*, December 2, 2022.
 - k. M-23-07, *Update to Transition to Electronic Records*, December 23, 2022.

(3) Other Federal Guidance.

- a. The Federal Information Security Modernization Act of 2014 (FISMA) (Pub. L. No. 113-283, Title II), December 2014, amended the Federal Information Security Management Act of 2002 (FISMA) to: (1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and (2) set forth authority for the Secretary of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems.
- b. The President's Identity Theft Task Force created a strategic plan to combat identity theft. The documents are available on the *Federal Trade Commission* website under **News and Events/Press Releases** at <https://www.ftc.gov/news-events/press-releases/2007/04/presidents-identity-theft-task-force-releases-comprehensive>. See The President's Identity Theft Task Force Report, *Combating Identity Theft: A Strategic Plan*, (April 2007), and The President's Identity Theft Task Force Report, *Combating Identity Theft, Volume II: Supplemental Information*, (April 2007), both located at <https://www.ftc.gov/reports/combating-identity-theft-strategic-plan>, and *The President's Identity Theft Task Force Report*, September 2008, <https://www.ftc.gov/sites/default/files/documents/reports/presidents-identity-theft-task-force-report/081021taskforcereport.pdf>.
- c. Treasury Directive 85-01, *Department of the Treasury Information Technology (IT) Security Program*, dated March 10, 2008, <https://home.treasury.gov/about/general-information/orders-and-directives/td85-01>, authorized the issuance of Treasury Department Publication (TD P) 85-01, *Treasury Information Technology Security Program*, which contains Department-wide IT security requirements and supporting guidance. Per TD P 85-01, dated December 12, 2017, "The primary purpose of the Treasury IT Security Program is to establish comprehensive, uniform cybersecurity policies and standards for the protection of Departmental assets. The IT Security Program serves as a foundation for the bureaus to use for their cybersecurity programs and in developing supplemental, bureau-specific policies, requirements, and operating directives." See also *TD P 85-01 Appendix A, Minimum Standard Parameters for Non-National Security Information and Information Systems*.
- d. Treasury Directive 25-08, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, dated December 22, 2009, <https://home.treasury.gov/about/general-information/orders-and-directives/td25-08>, established the Department of the Treasury's PII protection and breach response and notification policy and plan. This directive also authorized the issuance of a handbook or other guidance to implement this policy.
- e. Treasury's *Departmental Incident Response Plan*, dated October 10, 2018, established Departmental incident response (IR) procedures. Section 1.4, Authority Establishment, states, "IR procedures for addressing incidents concerning a breach of personally identifiable information (PII) are established in accordance with OMB-M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*."

(4) IRS IRMs.

- a. IRM 10.5.1, *Privacy and Information Protection, Privacy Policy*

- b. IRM 10.5.5, *Privacy and Information Protection, Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance and Requirements*
- c. IRM 1.15, *Records and Information Management*
- d. IRM 11.3, *Disclosure of Official Information*
- e. IRM 10.5.6, *Privacy and Information Protection, Privacy Act*
- f. IRM 1.1.27, *Organization and Staffing, Privacy, Governmental Liaison and Disclosure (PGLD)*

- (5) **Publicly available external websites and publications.** The publicly available external websites and publications listed in the table below provide general information on identity theft and identity theft-related issues.

#	Title	Description	Link	Owner
1	IRS Website	IRS Identity Theft Central	https://www.irs.gov/identity-theft-central	IRS
2	IRS Website	Taxpayer Guide to Identity Theft	https://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft	IRS
3	Federal Trade Commission (FTC) Identity Theft Website	Prevention tips and free resources.	https://consumer.ftc.gov/features/identity-theft	FTC
4	Federal Trade Commission (FTC) Identity Theft Website	IdentityTheft.gov is the federal government's one-stop resource for identity theft victims. The site provides streamlined checklists and sample letters to guide taxpayers through the recovery process. It also allows taxpayers to file Form 14039 online.	https://www.identitytheft.gov/	FTC
5	Federal Trade Commission (FTC) data breach information	Specific guidance for data breaches involving SSNs, payment card information, bank accounts, driver's licenses; children's information, and account credentials.	https://www.identitytheft.gov/Info-Lost-or-Stolen	FTC
6	IRS Form 14039, <i>Identity Theft Affidavit</i>	Direct link to IRS Identity Theft Affidavit (Form 14039). This form is used by taxpayers who want to report to the IRS that someone used their information to file taxes or to report that they are a victim of identity theft.	https://www.irs.gov/pub/irs-pdf/f14039.pdf	IRS

#	Title	Description	Link	Owner
7	United States Department of Justice Website	Identity Theft and Identity Fraud Information	https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud	DOJ
8	Taxpayer Advocate Service (TAS) Website	Taxpayer Advocate Service home page	https://www.irs.gov/advocate	TAS
9	Social Security Administration (SSA) Website	Social Security Administration (SSA) home page	https://www.ssa.gov	SSA
10	Social Security Administration (SSA) Publication No. 05-10064: Identity Theft and Your Social Security Number	Social Security Administration (SSA) Publication	https://www.ssa.gov/pubs/EN-05-10064.pdf	SSA
11	Identity Theft Task Force Webpage on the Federal Trade Commission (FTC) Website	Federal Trade Commission website/News and Events/ Press Releases/President's Task Force on Identity Theft	https://www.ftc.gov/news-events/press-releases/2007/04/presidents-identity-theft-task-force-releases-comprehensive	Identity Theft Task Force
12	IRS Phishing Website	Instructions on how to report and identify phishing, email scams, and bogus IRS websites	https://www.irs.gov/uac/report-phishing	IRS
13	Credit Bureaus/ Credit Reporting Agencies	Direct links to the three major credit bureaus/credit reporting agencies: Equifax, Experian, and TransUnion	http://www.equifax.com http://www.experian.com http://www.transunion.com/	Equifax, Experian, and TransUnion
14	IRS Pub 4524	Security Awareness for Taxpayers	https://www.irs.gov/pub/irs-pdf/p4524.pdf	IRS
15	IRS Pub 5027	Identity Theft Information for Taxpayers	<ul style="list-style-type: none"> • English https://www.irs.gov/pub/irs-pdf/p5027.pdf • Spanish https://www.irs.gov/pub/irs-pdf/p5027sp.pdf 	IRS
16	Identity Theft Resource Center® (ITRC) Website	Nonprofit organization dedicated exclusively to the understanding and prevention of identity theft	http://www.idtheftcenter.org/	ITRC

#	Title	Description	Link	Owner
17	Federal Trade Commission (FTC) Identity Theft Website. Online Privacy and Security/ Consumer Advice (ftc.gov)	Understanding online privacy, how to protect your devices from hackers and threats, and how to avoid common online scams.	https://consumer.ftc.gov/identity-theft-and-online-security/online-privacy-and-security	FTC
18	IRS Pub 1075	Tax Information Security Guidelines for Federal, State and Local Agencies	https://www.irs.gov/pub/irs-pdf/p1075.pdf	IRS

- (6) **Internal IRS intranet links.** The internal IRS intranet links listed in the table below provide information on identity theft, identity theft-related issues, and data breaches.

#	Title	Description	Link	Owner
1	Disclosure and Privacy Knowledge Base Site	Disclosure and Privacy homepage in the Disclosure and Privacy Knowledge Base Site	<i>Disclosure and Privacy Knowledge Base Site (Internal Link)</i>	PGLD
2	Disclosure and Privacy Knowledge Base Site, Report Losses, Thefts or Disclosures page	Report Losses, Thefts or Disclosures of Sensitive Data; Report Lost or Stolen IT Assets and BYOD Assets page in the Disclosure and Privacy Knowledge Base Site	<i>Report Losses, Thefts or Disclosures page (Internal Link)</i>	PGLD
3	Privacy, Governmental Liaison and Disclosure (PGLD) e-Trak Privacy online application	Privacy, Governmental Liaison and Disclosure (PGLD) PII Breach Reporting Form	<i>PII Breach Reporting Form (Internal Link)</i>	PGLD
4	Privacy, Governmental Liaison and Disclosure (PGLD) If/Then Guide for Reporting Incidents and Breaches	Privacy, Governmental Liaison and Disclosure (PGLD) If/Then Guide (pdf) for Reporting Incidents and Data Breaches in the Disclosure and Privacy Knowledge Base Site	<i>If/Then Guide for Reporting Incidents and Data Breaches (Internal Link)</i>	PGLD

#	Title	Description	Link	Owner
5	Computer Security Incident Response Center (CSIRC) Website	Computer Security Incident Response Center (CSIRC) Computer Security Incident Reporting Form	<i>CSIRC Computer Security Incident Reporting Form</i> (Internal Link)	IT (Information Technology)
6	Situational Awareness Management Center (SAMC)	Situational Awareness Management Center (SAMC) Incident Reporting Link for Reporting Physical Security Incidents	<i>(SAMC) Incident Reporting Link</i> (Internal Link)	SAMC
7	IRM 1.2.1, <i>Service-wide Policies and Authorities, Service-wide Policy Statements</i>	Policy Statement 10-1 (formerly P-25-1), IRS Policy Statement on assisting taxpayers who report they are victims of identity theft	IRM 1.2.1	IRS
8	IRM 25.23, <i>Identity Protection and Victim Assistance</i>	Identity Protection and Victim Assistance IRMs	IRM 25.23	IRS

10.5.4.2
(10-22-2019)
Awareness Training and Education

- (1) The Incident Management Program develops and implements initiatives to inform IRS personnel of their responsibilities for protecting taxpayers and employees against the loss, theft, or inadvertent unauthorized disclosure of SBU data, including PII and tax information.

Note: Failure to properly protect SBU data, including PII and tax information, can result in disciplinary actions including admonishment, written reprimand, suspension or removal.

- (2) The Incident Management Program supports the annual Privacy, Information Protection and Disclosure Mandatory Briefing, the Unauthorized Access (UNAX) Mandatory Briefing, and the Records Management Mandatory Briefing which are all managed by PGLD. These briefings provide information about privacy, disclosure, records management, computer security, and UNAX to all employees.

10.5.4.3
(10-07-2020)
Reporting Losses, Thefts and Disclosures

- (1) All IRS personnel are required to report the loss or theft of an IRS IT asset, or an asset in the *Bring Your Own Device (BYOD)* program, or hardcopy record or document containing SBU data, including PII and tax information, or the inadvertent unauthorized disclosure of SBU data, including PII and tax information, whether it be electronically, verbally or in hardcopy form, **immediately upon discovery**.

Note: SBU data includes, but is not limited to, taxpayer correspondence, tax information, tax returns, transcripts, faxes, email messages, passwords, sensitive

guidance, and personnel and job application information. See IRM 10.5.1.2.2.1, *Examples and Categories of SBU Data*, for additional information and examples.

- (2) All IRS personnel, including contractors and their employees, must be aware of their responsibilities under the law to safeguard SBU data, including PII and tax information, the procedures to follow when data is lost or compromised and the penalties for unauthorized disclosure of SBU data, including PII and tax information. Contractors should refer to the *Contractor Security Information* page on irs.gov, <https://www.irs.gov/about-irs/procurement/contractor-security-information>, Pub 4465-A, *Protecting Federal Tax Information for Contractors*, and Pub 4812, *Contractor Security and Privacy Controls*, for information about a contractor's responsibilities to protect Federal Tax Information (FTI) and incident/data breach response and reporting procedures.

10.5.4.3.1
(03-02-2023)

**Timely Reporting:
Immediately Upon
Discovery**

- (1) All IRS data breaches involving SBU data, including PII and tax information, and all suspected security incidents, including any incidents of loss or mishandling of IRS information technology resources and lost or stolen IRS IT assets and BYOD assets, must be reported **immediately upon discovery**.

Note: The reporting time frame was updated from "within one hour" to "immediately upon discovery," beginning with the October 2019 publication of this IRM to comply with the reporting time frame language in TD P 85-01, Appendix A, Minimum Standard Parameters for Non-National Security Information and Information Systems.

- (2) The timely reporting of all erroneous taxpayer correspondence involving the disclosure of SBU data, including PII and tax information, all inadvertent unauthorized disclosures of SBU data, including PII and tax information, all losses or thefts of hardcopy records or documents containing SBU data, including PII and tax information, and all suspected security incidents, including any incidents of loss or mishandling of IRS information technology resources and lost or stolen IRS IT assets and BYOD assets, is critical for quickly initiating any needed investigation or recovery of information **by the BU data owner**. A prompt report decreases the possibility the information will be compromised and used to perpetrate identity theft or other forms of harm. See IRM 10.5.4.4.4, *PGLD/Incident Management Risk Assessment*, and Exhibit 10.5.4-1, *Glossary of Incident Management Terms, Definitions, and Acronyms*, for additional information about, and examples of, **harm/risk of harm**. See IRM 10.5.4.1.3, *Responsibilities*, and the *Incident/Data Breach Responsibilities for Reporting Employees and Business Unit (BU) Data Owners* page in the Disclosure and Privacy Knowledge Base Site for additional information about the actions BU data owners must take in regard to containing data leakage and mitigating risk, or contact PGLD/IM via the *PII mailbox for additional mitigation guidance and assistance.

10.5.4.3.2
(10-07-2020)

**Intentional Unauthorized
Disclosures of Tax
Information**

- (1) Data breaches involving *intentional unauthorized disclosures* of SBU data, including PII and tax information, must be reported to the Treasury Inspector General for Tax Administration (TIGTA). See IRM 11.3.38.5, *Reporting Suspected Willful Unauthorized Accesses or Disclosures*, for additional information. See also IRC 7213, **Unauthorized Disclosure Of Information**, which imposes fines and/or other punishment for the willful unauthorized disclosure of a return or return information.

10.5.4.3.3
(03-02-2023)

**Inadvertent
Unauthorized
Disclosures and Losses
or Thefts of IT Assets,
BYOD Assets and
Hardcopy
Records/Documents**

- (1) It is critical to report an incident/data breach as soon as actionable information is available so a response/reaction can be initiated. Incident/data breach updates and any additional notifications to TIGTA and/or Law Enforcement (see (3) and (4) below) can be completed after the initial report to the Office of Privacy, Governmental Liaison and Disclosure/Incident Management Office (PGLD/IM), the Situational Awareness Management Center (SAMC), or the Computer Security Incident Response Center (CSIRC) is submitted.
- (2) **IRS employees are required to report incidents and data breaches *immediately upon discovery* to their manager and to one of the following offices based on what was lost, stolen, destroyed, or disclosed:**

- a. **The Office of Privacy, Governmental Liaison and Disclosure (PGLD) Incident Management Office (IM).** Report the data breach to PGLD/IM using the *PII Breach Reporting Form* if the data breach involves: erroneous taxpayer correspondence involving the disclosure of SBU data, including PII and tax information, i.e., a notice, letter, or transcript, which was mailed, emailed, faxed, EEFaxed, or generated or transmitted via the Income Verification Express Service (IVES), Return and Income Verification Services (RAIVS), Transcript Delivery System (TDS), Secure Data Transport (SDT), or other electronic transmission, to the wrong address or addressee; **or** notices, letters, transcripts, faxes, or other electronic/digital documents sent with mixed entity information such as correct taxpayer information is on page one, but unrelated taxpayer information is on page two; two letters for different taxpayers in the same envelope; the attachment in the correspondence is for a different taxpayer, etc.; **or** an inadvertent unauthorized disclosure of SBU data, including PII and tax information, such as a verbal disclosure, or an email sent to the wrong person or not properly encrypted; **or** the loss, theft, or unauthorized destruction of documents containing SBU data, including PII and tax information, such as hardcopy records, documents, or case files, packages lost or stolen during UPS or FedEx shipment, or lost or stolen remittances; **or** an electronic disclosure of SBU data, including PII and tax information, in IRMs, Training Materials, PowerPoints, IRS Source, SharePoint, etc., or on external systems/sites such as WhatsApp, GitHub, etc.

Note: Call 267-466-0777, or email Incident Management's **PII mailbox*, if you have any problems with the online PII Breach Reporting Form or any questions about completing the online form.

Note: In addition to the reporting requirement to PGLD/IM, data breaches involving disclosures of SBU data, including PII and tax information, in IRMs, must also be reported to the Office of Servicewide Policy, Directives and Electronic Resources (SPDER) via the **SPDER mailbox*.

Note: The loss, theft, or unauthorized destruction of official records (whether the records contain PII or not), in hardcopy or electronic format, are also reported via the *PII Breach Reporting Form*. PGLD/IM reviews all PII Breach Reporting Forms and alerts the **Records and Information Management (RIM) Program Office** if official records have been reported as lost, stolen, or destroyed on the PII Breach Reporting Form in accordance with IRM 1.15.3.4, *Unauthorized Disposition of Records*, and 36 CFR 1230, *Unlawful or Accidental Removal, Defacing, Alteration, or Destruction of Records*. Upon notification of the Records Loss Report from the IM office, the RIM Program office will contact the reporting point of contact to complete Form 15035, *Re-*

Records Loss Reporting. The RIM Program office will then conduct an intake and risk assessment process. See IRM 1.15.3, *Records and Information Management, Disposing of Records*; visit the *Records Management* page in the *Disclosure and Privacy Knowledge Base Site*; or contact the *RIM staff* at RIM's **Records Management mailbox* for additional information about records.

Note: See (3) and (4) below and the *If/then Guide for Reporting Incidents and Data Breaches* (PDF) for additional reporting requirements based on what was lost, stolen, destroyed, or disclosed.

- b. **The Situational Awareness Management Center (SAMC).** Report the incident to SAMC (within 30 minutes) using the *Incident Reporting Link* and selecting the button, **Report a New Physical Incident**, if the incident involves the loss or theft of Identification (ID) Media, including SmartID cards, Physical Access Control (PAC) cards, Pocket Commissions (credentials), etc., building access cards, building or room keys, legacy ID cards, government property or equipment, or physical security incidents and/or threats. See IRM 10.2.5, *Physical Security Program, Identification Media*, and IRM 10.2.8, *Physical Security Program, Incident Reporting*, or visit the Facilities Management and Security Services *FMSS Incident Reporting* page for additional reporting requirements and to learn more about FMSS and SAMC.

Note: See the *If/then Guide for Reporting Incidents and Data Breaches* (PDF) to check for additional reporting requirements based on what was lost, stolen, destroyed, or disclosed.

- c. **The Computer Security Incident Response Center (CSIRC).** Report the incident/data breach to CSIRC using the *Computer Security Incident Reporting Form*, or by calling CSIRC at 240-613-3606, if the incident/data breach involves: the loss or mishandling of IRS information technology resources; **or** the loss or theft of an IRS IT asset, e.g., an IRS issued computer, laptop, router, printer, cell phone, BlackBerry, or removable storage media (CD/DVD, flash drive, floppy, etc.); **or** the loss or theft of a non-government furnished/personally owned mobile device that accesses, processes, transmits, or stores IRS information, in support of the Bring Your Own Device (BYOD) program; **or** an IRS IT asset or BYOD asset lost or stolen during UPS or FedEx shipment.

Note: If the incident/data breach involves the loss or theft of multiple assets, i.e., an IRS IT asset, or BYOD asset, **and** hardcopy records or documents containing SBU data, including PII and tax information, **report the incident/data breach to CSIRC.** Do not report it to PGLD/IM.

Note: All suspected security incidents, including any incidents of loss or mishandling of IRS information technology resources and lost or stolen IRS IT assets and BYOD assets, must be reported to CSIRC **immediately upon discovery.**

Note: See (3) and (4) below and the *If/then Guide for Reporting Incidents and Data Breaches* (PDF) for additional reporting requirements based on what was lost, stolen, destroyed, or disclosed.

- (3) **The Treasury Inspector General for Tax Administration (TIGTA).** Report the incident/data breach to TIGTA by calling 800-366-4484, if the incident/data breach involves: the loss or theft of an IRS IT asset, e.g., an IRS issued

computer, laptop, router, printer, cell phone, removable storage media (CD/DVD, flash drive, floppy, etc.); **or** the loss or theft of a non-IRS IT asset (BYOD device); **or** an IRS IT asset or BYOD asset lost or stolen during UPS or FedEx shipment; **or** the loss, theft, or unauthorized destruction of official records (whether the documents contain PII or not); **or** the loss, theft, or unauthorized destruction of documents containing SBU data, including PII and tax information, such as hardcopy records, documents, or case files, packages lost or stolen during UPS or FedEx shipment, or lost or stolen remittances.

- (4) **Local Law Enforcement.** Report the incident/data breach to your local Law Enforcement authority and file a Police Report if the incident/data breach involves a theft, but do not disclose sensitive data and/or taxpayer data.
- (5) **Treasury Shared Services Security Operations Center (TSSSOC).** The *applicable reporting office* – **either PGLD/IM or CSIRC** – will report to the Treasury Computer Security Incident Response Center (TCSIRC) for further submission to TSSSOC as necessary.
 - a. CSIRC will report incidents to TCSIRC for assessment and reporting to the United States Computer Emergency Readiness Team (US-CERT) as necessary.
 - b. For data breaches reported to PGLD/IM through the online reporting tool, IM will report to TCSIRC data breaches meeting Treasury’s reporting requirements.
 - c. The PPC Director in PGLD will coordinate with Treasury when additional reporting may be required to law enforcement, oversight entities, or Congress.
- (6) Visit the *Report Losses, Thefts or Disclosures* page in the Disclosure and Privacy Knowledge Base Site and see the ***If/Then Guide for Reporting Incidents and Data Breaches (PDF)*** listed in the **Other Related Resources** section for additional information and guidance. If you are a Flexiplace (Telework) employee (Frequent, Recurring or Ad Hoc) or a Mobile employee, print a copy of the If/Then Guide for the office and one to keep at home in case your IRS IT asset or BYOD asset is lost or stolen, and you can’t access IRS Source.

10.5.4.3.4
(03-02-2023)
**Inadvertent Accesses of
Tax Information**

- (1) Inadvertent accesses of taxpayer information are reported on the hard copy Form 11377, *Taxpayer Data Access*, or the fillable Form 11377-E, *Taxpayer Data Access*.
- (2) Form 11377 or Form 11377-E may be used by employees Servicewide to document accesses to taxpayer return information when the accesses are not supported by direct case assignment, were performed in error (inadvertent access), or when the access may raise a suspicion of an unauthorized access.
- (3) Some examples of an inadvertent access include accidentally entering an incorrect Taxpayer Identification Number or unintentionally retrieving other taxpayer information while working an assigned case. Inadvertent accesses are not reported to PGLD/IM or CSIRC.
- (4) Employees who complete either the online or printed version of this form are required to sign and date the IRS and Employee copies and give both to their managers no later than the end of the workday that the accesses occurred.

The manager will review the form, sign and date both copies and return the Employee Copy to the employee. Employees are encouraged to retain their copy for six years.

10.5.4.3.5
(03-02-2023)
“No Reporting”
Situations

- (1) The following are examples of situations which require no reporting to PGLD/IM as they are not considered erroneous taxpayer correspondence or *unauthorized disclosures*:
- a. An IRS employee follows all procedures to verify the identity of a caller before disclosing any information, only to later find that he or she is not talking to the taxpayer or the taxpayer’s authorized representative. The employee terminates the call at that point without disclosing any further information.
 - b. An IRS employee faxes return information as requested by a taxpayer or authorized representative. The employee follows all established procedures for faxing SBU data, including PII and tax information, only to later find that the fax number provided by the taxpayer or authorized representative was incorrect.
 - c. An IRS employee follows all established procedures for locating a potential new address for a taxpayer, and a letter is generated to that address in an attempt to contact the taxpayer. A person who receives the correspondence at that address contacts the IRS to say the individual does not live there.
 - d. The IRS sends correspondence to the last known address of a taxpayer. A person who receives the correspondence at that address contacts the IRS to say the individual does not live there.
 - e. An IRS employee follows procedures in IRM 21.1.3.12, *Suicide Threats*, to disclose a taxpayer’s name, address/location, and/or telephone number to Law Enforcement because the taxpayer threatened suicide and/or threatened harm to another individual. In this situation, the disclosure of this information is not prohibited by law; therefore, although the Suicide Threat must be reported to Disclosure, TIGTA, SAMC, and the Office of Employee Protection, no reporting to PGLD/IM is necessary unless directed to do so by Disclosure. See IRM 21.1.3.12, *Suicide Threats*, IRM 10.2.8, *Physical Security Program, Incident Reporting*, IRM 11.3.34.3, *Expedited Procedures in Emergency Situations*, and the Governmental Liaison, Disclosure and Safeguards (GLDS) *Unique Situations* page for the procedures to follow when a taxpayer threatens suicide or when it is appropriate to contact the local Law Enforcement authority versus federal or State Law Enforcement authorities.
- Note:** Visit the *Report Losses, Thefts or Disclosures* page in the Disclosure and Privacy Knowledge Base Site and see the **No Reporting Situations (PDF)** listed in the **Other Related Resources** section for additional information and guidance.

10.5.4.4
(10-19-2017)
PGLD/Incident
Management Intake,
Risk Assessment and
Notification

- (1) This section covers the intake and risk assessment of IRS data breaches by PGLD/IM as well as notification to potentially impacted individuals.

10.5.4.4.1
(03-02-2023)
**PGLD/Incident
Management Intake**

- (1) When an IRS data breach or incident occurs, depending on what was lost, stolen, destroyed, or disclosed, employees report the data breach or incident to PGLD/IM via the PII Breach Reporting Form, to CSIRC via the Computer Security Incident Reporting Form, or to SAMC via SAMC's Incident Reporting Link.
- a. A data breach is reported to PGLD/IM via PGLD's *PII Breach Reporting Form* if the data breach involves erroneous taxpayer correspondence involving the disclosure of SBU data, including PII and tax information, i.e., a notice, letter, or transcript, which was mailed, emailed, faxed, EEFaxed, or generated or transmitted via IVES, RAIVS, TDS, SDT, or other electronic transmission, to the wrong address or addressee; **or** notices, letters, transcripts, faxes, or other electronic/digital documents sent with mixed entity information such as correct taxpayer information is on page one, but unrelated taxpayer information is on page two; two letters for different taxpayers in the same envelope; the attachment in the correspondence is for a different taxpayer, etc.; **or** an inadvertent unauthorized disclosure of SBU data, including PII and tax information, such as a verbal disclosure, or an email sent to the wrong person or not properly encrypted; **or** the loss, theft, or unauthorized destruction of documents containing SBU data, including PII and tax information, such as hardcopy records, documents, or case files, packages lost or stolen during UPS or FedEx shipment, or lost or stolen remittances; **or** an electronic disclosure of SBU data, including PII and tax information, in IRMs, Training Materials, PowerPoints, IRS Source, SharePoint, etc., or on external systems/sites such as WhatsApp, GitHub, etc.

Note: The **PII Breach Reporting Form** is a web-based online reporting form that uploads directly to e-Trak.

Note: **Form 14164, Personally Identifiable Information (PII) Analysis**, is auto-populated through e-Trak based on the information the reporting employee enters on the e-Trak online breach reporting form (PII Breach Reporting Form). Form 14164 is generated for informational purposes to provide reporting employees with a summary of their responses from the e-Trak online breach reporting form for their records. **Form 14164 is viewable from the Publishing Catalog, but it is not fillable.**

- b. An incident/data breach is reported to CSIRC via CSIRC's *Computer Security Incident Reporting Form* if the incident/data breach involves the loss or mishandling of IRS information technology resources, **or** the loss or theft of an IRS IT asset or an asset in the Bring Your Own Device (BYOD) program, **or** an IRS IT asset or BYOD asset lost or stolen during UPS or FedEx shipment, **or** if it involves multiple assets, i.e., an IRS IT asset or BYOD asset **and** hardcopy records or documents containing SBU data, including PII and tax information. Note that the form and instructions for incidents/data breaches involving IT assets are different from the forms and instructions for all other data breaches.
- c. An incident is reported to SAMC via SAMC's *Incident Reporting Link* if the incident involves the loss or theft of ID media, including SmartID cards, PAC cards, Pocket Commissions (credentials), etc., building access cards, building or room keys, legacy ID cards, government property or equipment, or physical security incidents and/or threats. Note the reporting requirement time frame for SAMC is within **30 minutes** of discovery.

- (2) After a data breach is reported, PGLD/IM receives notification via email (delivered to the *PII mailbox) from either CSIRC or e-Trak. The email contains the information necessary to conduct a risk assessment and to determine if the data breach meets high-risk data breach criteria.
- a. The *PII mailbox is a centralized communication tool used by PGLD/IM to send and receive all communications throughout the data breach intake process. Data breach summaries with a brief description of the data breach are automatically sent via email to the *PII mailbox whenever data breaches are reported to CSIRC via the Computer Security Incident Reporting Form or to PGLD/IM via the PII Breach Reporting Form.

Note: Incident Management Intake may also include events received from SPIIDE for investigation.

- (3) After PGLD/IM reviews the information submitted and performs an initial assessment of the data breach, if SBU data, including PII and tax information, is involved, PGLD/IM will, if necessary, request additional information to fully assess the data breach to complete the risk assessment. If the data breach is input through the e-Trak online breach reporting form (PII Breach Reporting Form) and the employee indicated an SSN or EIN was disclosed, the reporting employee and the employee's manager will receive an *Impacted Individuals and/or Business Excel Spreadsheet* as an attachment to the email received from e-Trak. If the data breach is input through other than the e-Trak online reporting form, PGLD/IM will send an *Impacted Individuals Excel Spreadsheet* to the reporting employee and the employee's manager if an SSN is needed for notification. The reporting employee is responsible for providing the **complete, unredacted tax identification numbers (SSNs/EINs)** of the potentially impacted individuals and/or businesses and emailing the spreadsheet via secure email to the *PII mailbox **within two business days of receipt**.

Note: If the unredacted (not truncated) SSNs for the potentially impacted individuals involved in the data breach are not readily available, the Reporting Employee or BU data owner must research to determine the complete SSNs. After due diligence, if the unredacted SSNs for the potentially impacted individuals cannot be determined, email the *PII mailbox, or contact IM at 267-466-0777.

- a. The PGLD/IM and CSIRC Breach/Incident Reporting Forms provide an inventory of possible compromised data elements, the source of the data, whether the data was encrypted, and any other special factors that need to be considered, such as data being used in a criminal or grand jury investigation.
- b. The *Impacted Individuals and/or Business Excel Spreadsheet* provides an inventory of the names and TINs of all the individuals potentially impacted by the data breach.

10.5.4.4.2 (09-02-2022)

High-Risk Data Breaches

- (1) A high-risk data breach includes any data breach that meets the OMB definition of a major incident or includes any special circumstances requiring an enhanced response because of significant risk to:
- a. **Customers:** Affects a significant number of individuals or high-profile individuals;

- b. **Business Results:** Overwhelming increase of phone traffic, reduced taxpayer access to IRS systems or online applications, negative affect on revenue protection; or,
 - c. **IRS Reputation:** Potential for extensive media involvement, congressional interest, or negative exposure.
- (2) High-risk data breaches may be identified through several different channels. For example:
- a. Cybersecurity may identify a potential breach of an IRS system or application.
 - b. PGLD or another BU may identify a loss, theft, or disclosure of SBU data, including PII and tax information, with unusual circumstances.
 - c. A third-party data owner may identify a breach of SBU data, including PII and tax information.
- Note:** A third-party data owner is defined as a data owner external to the IRS. An external third-party data breach is an event that results from the unauthorized use or loss of SBU data (including PII and tax information) that does not involve IRS systems, applications, or online services. Third-party data breaches can be reported to the IRS by external sources, such as practitioners, software developers, state and local agencies, or others.
- (3) BU data owners will:
- a. Notify PGLD and IRS senior management as needed.
 - b. Take immediate action to contain potential data leakage and mitigate risk, such as engaging Cybersecurity's Online Fraud Detection and Prevention (OFDP) Office to deactivate a fraudulent website; recovering hardcopy documents; or coordinating with TIGTA to ensure all recovery options are considered.
- (4) PGLD will:
- a. Identify members needed for a Breach Response Team (BRT) or Working Group (WG).
 - b. Notify the Department of Treasury as applicable.
- (5) A Breach Response Team (BRT) will be convened for high-risk data breaches and for any data breach that constitutes a major incident (as defined in OMB guidance) to address the additional concerns and communication issues that may be involved with these types of data breaches. The purpose of the BRT is to provide a swift, effective and orderly response to these types of data breaches. The team is led by the Breach Coordinator (BC) and is composed of cross-functional representatives authorized to take the necessary steps to contain, mitigate or rectify a data breach, mitigate the vulnerability of taxpayer data, and rebuild trust. Participating members of the BRT can vary based on the nature and scope of the data breach and the potential risk to taxpayers.
- (6) A Working Group (WG) is comprised of members from several different components of a BRT to address the specifics of an investigation prior to the formation of a full BRT. WGs are commonly formed for investigations into suspicious behavior on IRS systems and applications.
- (7) PGLD/IM reports high-risk data breaches to the Facilities Management and Security Services (FMSS) Threat and Incident Response Center (TIRC). The

TIRC is comprised of staff from FMSS, the Treasury Inspector General for Tax Administration-Criminal Intelligence and Counterterrorism Group (TIGTA-CICT), Criminal Investigation (CI), Federal Protective Service (FPS), the Computer Security Incident Response Center (CSIRC), and the Office of Privacy, Governmental Liaison and Disclosure (PGLD), including the Records and Information Management (RIM) Program Office. The mission of the TIRC is to identify and mitigate threats and record countermeasures and mitigation strategies as it pertains to Federal tax administration and the IRS for the protection of service operations. Reporting to SAMC may also be required if the reporting does not lead to SAMC Leadership messaging and communication is warranted based on the circumstances of the event.

- (8) See the following resources regarding high-risk data breaches. Both are listed in the **Other Related Resources** section of the *Report Losses, Thefts or Disclosures* page in the Disclosure and Privacy Knowledge Base Site.
 - a. The High-Risk Data Breach Quick Reference Guide contains the high-level process to follow when a high-risk data breach is identified.
 - b. Document 13347, *Data Breach Response Playbook*, contains detailed procedures on the proper steps to take if your area has a high-risk data breach to help you minimize harm to taxpayers, document the data breach, and manage the risk assessment process.

10.5.4.4.3
(10-07-2020)
OMB Major Incidents

- (1) FISMA 2014 requires OMB to define the term “major incident” and directs agencies to report major incidents to Congress within 7 days of identification.
- (2) A “major incident,” as defined by OMB Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*, <https://www.whitehouse.gov/wp-content/uploads/2022/12/M-23-03-FY23-FISMA-Guidance-2.pdf>, is “any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people.”
- (3) A data breach constitutes a “major incident” when it involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. An unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to 100,000 or more individuals’ PII constitutes a **major incident**.
- (4) PGLD/IM coordinates with Treasury for the appropriate actions and reporting, including reporting to Congress, whenever a data breach is identified as an OMB major incident.

10.5.4.4.4
(03-02-2023)
**PGLD/Incident
Management Risk
Assessment**

- (1) PGLD/IM assesses the risk of harm to individuals potentially impacted by data breaches involving the loss, theft, or inadvertent unauthorized disclosure of SBU data, including PII and tax information. When assessing the risk of harm to individuals potentially impacted by a data breach, the potential harms that could result from the loss or compromise of PII must be considered. Such harms may include the effect of a breach of confidentiality or fiduciary responsibility, the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, financial harm, the disclosure of contact information for victims of abuse, the potential for secondary uses of the information which

could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem. Additionally, the Privacy Act requires the IRS to protect against any anticipated threats or hazards to the security or integrity of records which could result in **substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained**. The IRS must consider any and all risks relevant to the data breach, which may include risks to the IRS, IRS information systems, IRS programs and operations, other Treasury Bureaus, the Federal Government, or national security. These additional risks may properly influence the IRS' overall response to a data breach and the steps the IRS must take to notify individuals. Note that all data breaches are unique and when making determinations, all facts and circumstances must be considered.

- (2) PGLD/IM performs a risk assessment to evaluate the likely risk of harm for all reported IRS data breaches, based on standardized factors and ratings criteria. The result of the assessment is a categorization of the data breach into one of four levels - No Impact; Low Impact; Moderate Impact; and High Impact. Categorization into levels dictates a recommended level of response and determines when, what, how, and to whom notification of a data breach must be given.
- (3) PGLD/IM uses the following three-step methodology to assess the risk of harm for all reported IRS data breaches:
 - a. **Step 1: Examine key factors.** Each of the three factors identified by OMB Memorandum M-17-12 (the nature and sensitivity of the PII potentially compromised by the data breach; the likelihood of access and use of the PII potentially compromised by the data breach; and the type of data breach) is assessed in relation to the specific data breach to determine the potential likelihood of harm to individuals. See (4) below for additional information on the risk assessment factors.
 - b. **Step 2: Determine risk factor ratings.** Each of the three factors is rated based on its impact level (high, moderate, low, or no impact) with corresponding points from 3 to 0 assigned to each impact level.
 - c. **Step 3: Categorize or classify the data breach.** Based on the total factor rating points the data breach is categorized into one of four levels. Data breaches with a total factor rating point between 8 and 9 are considered Level Three (High Impact). Potentially impacted individuals involved in a data breach categorized as Level Three (High Impact) will be sent a data breach notification letter.
- (4) PGLD/IM considers the following key factors and considerations when conducting a risk assessment to determine the potential likelihood of harm to potentially impacted individuals. Identifying the data elements involved in the data breach, i.e., the PII that was lost, stolen, or disclosed, and assessing the impact of the data breach are key elements that must be considered when determining if, when, and how notification will be provided to potentially impacted individuals.
 - a. **Nature and Sensitivity of the PII.** The nature and sensitivity of the PII potentially compromised by the data breach, including the potential harms that an individual could experience from the loss or compromise of the type of PII. At a minimum, the following items are considered when assessing the nature and sensitivity of the PII potentially compromised by a data breach: **Data Elements**, including an analysis of the sensitivity of each individual data element as well as the sensitivity of all the data

- elements together; **Context**, including the purpose for which the PII was collected, maintained, and used; **Private Information**, including the extent to which the PII, in a given context, may reveal particularly private information about an individual or constitutes information that an individual would generally keep private; **Vulnerable Populations**, including the extent to which the PII identifies or disproportionately impacts a particularly vulnerable population; and **Permanence**, including the continued relevance and utility of the PII over time and whether the information is easily replaced or substituted or will permanently identify an individual.
- b. **Likelihood of Access and use of the PII.** The likelihood of access and use of the PII potentially compromised by the data breach, including whether the PII was properly encrypted, or rendered partially or completely inaccessible by other means. The following items are considered when assessing the likelihood of access and use of PII potentially compromised by a data breach: **Security Safeguards**, including whether the PII was properly encrypted, or rendered partially or completely inaccessible by other means; **Format and Media**, including whether the format of the PII or the media on which it is maintained may make it difficult and resource-intensive to use; **Duration of Exposure**, including how long the PII was exposed; and **Evidence of Misuse**, including any evidence confirming that the PII is being misused, or that it was never accessed.
- c. **Type of Data Breach.** The type of data breach, including the circumstances of the data breach, as well as the actors involved and their intent. The following items are considered when determining the type of data breach: **Intent**, including whether the PII was compromised intentionally, unintentionally, or whether the intent is unknown; and **Recipient**, including whether the PII was disclosed to a known or unknown recipient, and the trustworthiness of a known recipient.
- (5) After assessing the risk of harm to individuals potentially impacted by a data breach, PGLD/IM will determine how to best mitigate the identified risks. Because each data breach is fact-specific, the decision of whether to take countermeasures, offer guidance, or provide services to potentially impacted individuals will depend on the circumstances of the data breach. Actions the IRS can take to limit, reduce, or mitigate the risk of harm to potentially impacted individuals include:
- Countermeasures, such as placing markers on the accounts (e.g., identity theft markers and/or IRS Data Breach Tracking Indicator), ensuring the individuals are aware of the availability of the Identity Protection Personal Identification Number (IP PIN) for filing tax returns, or using database filters;
 - Guidance, such as providing individuals with information on how they may obtain a free credit report, how they may set up a fraud alert or place a credit freeze, and whether they should consider changing or closing certain accounts; and
 - Services, such as offering identity protection/identity monitoring or an IP PIN.
- (6) After IM has completed its risk analysis of a data breach and developed a recommendation regarding the appropriate response, data breaches categorized as “High Impact” are included in a Code Red Recommendations Report and presented to the Incident Management Associate Director for review.

- (7) If the recommendation is to notify, then potentially impacted individuals are notified of the data breach via *Letter 4281C, IM Breach Notification Letter*.

10.5.4.4.5
(08-29-2018)
The PII Working Group (PIIWG)

- (1) The PII Working Group (PIIWG) consists of senior management and technical experts from all key business and functional unit stakeholders with expertise in information technology, legal requirements, privacy, law enforcement and information security. A Code Red Recommendations Report is presented to the PIIWG weekly by PGLD/IM for information only; no concurrence or approval by the PIIWG is required.
- (2) The Privacy Policy and Compliance Advisory Committee (PPCAC) no longer exists. It was a committee comprised of executives from all key business and functional unit stakeholders. It was originally established to oversee the Identity Protection Program and Incident Management Program activities, specifically the development of Servicewide identity theft and data breach policies and procedures, development and execution of Identity Protection and Incident Management Program office procedures, and the study and execution of identity theft outreach, victim assistance and prevention initiatives.

10.5.4.4.6
(09-02-2022)
PGLD/Incident Management Data Breach Notification - Letter 4281C

- (1) The IRS, through PGLD/IM, will notify potentially impacted individuals if one of the following conditions occurs:
 - a. The evaluation of an IRS data breach results in a likelihood of harm to the potentially impacted individuals. See IRM 10.5.4.4.4, *PGLD/Incident Management Risk Assessment*, and Exhibit 10.5.4-1, *Glossary of Incident Management Terms, Definitions, and Acronyms*, for additional information about, and examples of, **harm/risk of harm**.
 - b. Personal information was intentionally accessed or disclosed without authorization if the access or disclosure results in an administrative proposal of disciplinary or adverse action against an IRS employee but not criminal indictment.
- (2) The IRS, through PGLD/IM, will notify potentially impacted individuals of an IRS data breach, or an intentional unauthorized access or disclosure resulting in proposed disciplinary or adverse action against an employee, via *Letter 4281C, IM Breach Notification Letter*.
- (3) The IRS, through PGLD/IM, will identify potentially impacted individuals of an IRS data breach who have been sent Letter 4281C by marking each entity (on CC ENMOD and/or CC IMFOLE) with the IRS data breach indicator TC 971 AC 505 (only if the account is on the Master File (MF)). A TC 971 AC 505 will only be input on the accounts of individuals who are sent Letter 4281C because of an intentional unauthorized access or disclosure if they are offered identity protections *such as* identity protection/identity monitoring services or IP PIN in the letter. If they are only advised of their rights under IRC 7431, **Civil Damages For Unauthorized Inspection Or Disclosure Of Returns And Return Information**, then no TC 971 AC 505 will be input. See IRM 10.5.4.5.1.1, *Applying the IRS Data Breach Tracking Indicator to IRS Data Breaches*, for additional information.
- (4) The objectives of communications in the event of a possible compromise of SBU data, including PII and tax information, within the IRS are as follows:
 - a. To comply with OMB and Treasury Department directives which mandate notification to potentially impacted individuals if there is a potential risk

that the compromised data may be used by someone other than the owner of the information to commit a crime or fraud.

- b. To comply with IRC 7431 when there is an unauthorized access or disclosure resulting in an administrative proposal of disciplinary or adverse action against an employee.
- c. To minimize the possible negative impact of the compromised data on the taxpayer/victim.
- d. To ensure the IRS' relationship with the impacted individual(s) will not be so damaged as a result of the data breach that it negatively impacts his or her tax filing and paying obligations.

10.5.4.4.6.1
(09-02-2022)

Contents of the Data Breach Notification Letter

- (1) The IRS will notify individuals potentially impacted by IRS data breaches (including intentional unauthorized accesses or disclosures resulting in proposed disciplinary or adverse action against an employee) using Correspondence *Letter 4281C, IM Breach Notification Letter*; however, the IRS may use a unique letter when deemed necessary and appropriate.

Note: These procedures apply only to data breach notifications and notifications to individuals whose personal information was intentionally accessed or disclosed without authorization resulting in an administrative proposal of disciplinary or adverse action against an employee; they do not apply to notifications made pursuant to 26 USC 7431(e), i.e., unauthorized access or disclosure resulting in a criminal indictment. See IRM 10.5.5, *Privacy and Information Protection, Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance and Requirements*.

- (2) Remedial services such as identity protection/identity monitoring services are offered to potentially impacted individuals of an IRS data breach as part of the overall OMB requirement regarding implementation of a data breach response program to mitigate the likely risk of harm, specifically the potential for identity theft.
- (3) Data breach notifications will be written plainly and clearly, and will generally include the following information:
 - a. A brief description of what happened, including the date of the data breach;
 - b. To the extent possible, a description of the type of PII disclosed as a result of the data breach (e.g., name, SSN, date of birth, address, etc.);
 - c. Actions that potentially impacted individuals should take to protect themselves from potential harm;
 - d. A toll-free telephone number that potentially impacted individuals can contact for more information;
 - e. A statement that the IRS has provided or will provide potentially impacted individuals with an identity protection/identity monitoring service at no cost (if the risk assessment results in a likelihood of harm, specifically the potential for identity theft (see (2) above), and the contact information for the vendor providing the service.

Note: The IRS does not auto-enroll potentially impacted individuals. The potentially impacted individual must contact the vendor to sign up for the free identity protection/identity monitoring service.

- (4) The data breach notification letter will also include rights under IRC 7431 and information on Low Income Taxpayer Clinics (LITCs) when there is an unau-

thorized access or disclosure resulting in an administrative proposal of disciplinary or adverse action against an employee.

- (5) The Privacy and Information Protection (PIP) toll-free telephone number provided in *Letter 4281C, IM Breach Notification Letter*, is **866-225-2009**. Individuals who call the PIP toll-free number are auto directed to the Identity Theft Product Line (Applications 161 and 162).

10.5.4.4.6.2
(08-29-2018)
Data Breach Notification Signature

- (1) The signature on the IRS data breach notification letter shall be that of the Privacy Policy and Compliance (PPC) Director.

10.5.4.4.6.3
(09-02-2022)
Timeliness of the Data Breach Notification

- (1) The IRS will notify individuals potentially impacted by IRS data breaches without unreasonable delay following the completion of the risk assessment process.

Note: The IRS has discretion to delay notification in cases where notification could adversely interfere with an ongoing criminal investigation or compromise national security and the delay will not increase the risk of harm to any potentially impacted individuals. See IRM 10.5.4.4.4, *PGLD/Incident Management Risk Assessment*, and Exhibit 10.5.4-1, *Glossary of Incident Management Terms, Definitions, and Acronyms*, for additional information about, and examples of, **harm/risk of harm**.

- (2) Business measures and lapse time goals were established to track/assess PGLD/IM and IRS performance. The FY23 measures and goals are:
 - a. **Measure 1: PPC Measure:** Lapse time (# of days) from Data Breach Report Date to the Data Breach Notification Letter Date. **Goal:** Median of 10 days or less.
 - b. **Measure 2: Enterprise Measure:** Lapse time (# of days) from the Data Breach Date to the Data Breach Notification Letter Date. **Goal:** Median of 24 days or less.
 - c. **Measure 3: OMB Measure:** Percentage of data breaches with a lapse time (# of days) of 30 days or less from the Data Breach Report Date to the Data Breach Notification Letter Date. **Goal:** Percentage of data breaches equal to or more than 94%. Measure 3 is reported to Treasury as part of OMB required reporting.

10.5.4.4.6.4
(03-02-2023)
Means of Providing Data Breach Notifications

- (1) The IRS will provide written notification to the individual's address of record on IDRS.
- (2) Based on the number of potentially impacted individuals and the urgency with which they may need to receive notice, the IRS may supplement written notification with other means of communication such as newspapers or other media outlets.
- (3) For high-risk data breaches, at the discretion of the BRT, and consistent with applicable law, the IRS may notify external entities. In making its decision, the BRT will consider whether notifying external entities would result in any of the following:

- a. Aiding the public in its response to the data breach (e.g., whether constructive notification via media channels would help the IRS alert potentially impacted individuals more effectively and expeditiously than via notification letter alone)
- b. Facilitating the IRS' ability to mitigate the potential harm resulting from the data breach (e.g., preparing counterpart entities such as the Federal Trade Commission (FTC) that may receive a surge in inquiries)
- c. Contributing to unnecessary public alarm
- d. Creating an unnecessary burden on the public, external entities, or potentially impacted individuals

10.5.4.4.7
(10-19-2017)
Ongoing Support

- (1) Based on the circumstances of the data breach, the IRS will provide ongoing support to potentially impacted individuals. This post-notification assistance and support may include, but is not limited to, the following:
 - a. A dedicated toll-free telephone number staffed by trained IRS personnel to respond to general data breach-related inquiries
 - b. Information on websites and other resources providing information about identity theft prevention and protection
 - c. Coordination with Business Units on IRS data breaches that affect an individual's tax account, such as phishing schemes
- (2) The PGLD/Incident Management Program is supported by Wage and Investment's (W&I) Accounts Management (AM). AM Customer Service Representatives (CSRs) support PGLD/IM by assisting individuals who call the Privacy and Information Protection (PIP) toll-free telephone number (866-225-2009) provided in *Letter 4281C, IM Breach Notification Letter*. AM CSRs are trained to respond to IRS data breach questions and questions about Letter 4281C.

10.5.4.4.7.1
(09-02-2022)
**Handling Inquiries About
IM Data Breach
Notification Letters**

- (1) These procedures apply to data breach notifications including notifications to individuals whose personal information was intentionally accessed or disclosed without authorization resulting in an administrative proposal of disciplinary or adverse action against an employee; they do not apply to notifications made pursuant to 26 USC 7431(e), i.e., unauthorized access or disclosure resulting in a criminal indictment. See IRM 10.5.5, *Privacy and Information Protection, Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance and Requirements*.
- (2) The contact telephone number provided in *Letter 4281C, IM Breach Notification Letter*, is 866-225-2009. The 4281C Letter does not require individuals to contact the IRS; however, some individuals may call with questions or concerns about the letter. Individuals who call the PIP toll-free number are auto directed to the Identity Theft Product Line (Applications 161 and 162).
- (3) In some instances, individuals who receive Letter 4281C may call an IRS telephone number other than the number provided in the letter (866-225-2009). If an IRS phone assistor other than an AM Customer Service Representative (CSR) receives a call from an individual in response to Letter 4281C, or the individual asks to speak to the employee whose number appears on Letter 4281C (0847999999), transfer the call to extension 1161 (for callers needing assistance in Spanish, use extension 1162).
- (4) AM CSRs answer general data breach-related inquiries about the IRS data breach and prepare a Form 4442, *Inquiry Referral*, if the caller requests

specific information about the data breach that the AM CSR is unable to answer. The Form 4442 is directed to PGLD’s IM office in Philadelphia for resolution. See IRM 10.5.4.4.7.6, *Referrals to PGLD’s Incident Management Office*.

- (5) Correspondence (and any attachments) received in response to Letter 4281C, or addressed to employee 0847999999, must be forwarded to the local Image Control Team (ICT) for scanning and controlling. See IRM Exhibit 3.10.72-2, *Correspondex C Letters - Routing Guide*; IRM Exhibit 3.13.6-1, *Appendix A - Document Types, Category Codes, IMF Domestic*; IRM Exhibit 3.13.6-14, *Appendix N - Document Types, Category Codes, Priority Codes, IDT - IMF*; and IRM 21.5.1.4.2.3, *Clerical Function for the Image Control Team (ICT) Correspondence Imaging System (CIS)*, for information about ICT. See IRM 21.5.1.5, *Correspondence Imaging System (CIS) Procedures*, for information about CIS procedures, and the *Image Control Team (ICT)* link in the Miscellaneous section of the Campus Program Locator Guide (located under the Who/Where tab) to determine the address for your local ICT function. **ICT will review the correspondence and determine if a Referral to the IM office in Philadelphia is necessary.**
 - a. If scanning is not available, route the correspondence and any attachments received in response to Letter 4281C, or addressed to employee 0847999999, to AM. See the address table below; IRM 10.5.1.6.9.3, *Shipping*; the PGLD *Shipping* page on the Disclosure and Privacy Knowledge Base Site; Document 13056, *Employee Toolkit: Shipping Procedures for Personally Identifiable Information (PII)*; and Document 13144, *Proper PII Shipping Procedures*, for policy and procedures relating to protecting and handling SBU data, including PII and tax information.
 - b. If the correspondence appears to be time sensitive, fax it to the Image Control Team (ICT) at 855-807-5720. ICT will review the correspondence and determine if a Referral to the IM office in Philadelphia is necessary.

United States Postal Service (USPS) Mailing Address	Private Delivery Service (PDS) Mailing Address
Internal Revenue Service Accounts Management Fresno, CA 93888-0025	Internal Revenue Service Accounts Management 3211 S Northpointe Dr, Fresno, CA 93725

- (6) See the *IRS Data Breach Frequently Asked Questions (FAQs)* on SERP for a list of frequently asked questions about Letter 4281C and general questions about IRS data breaches.

10.5.4.4.7.2
(08-29-2018)
**IMF Identity Check - AM
IDT Toll-Free (App
161/162) Telephone
Overview**

- (1) When taking calls from impacted individuals, a consistent and proper greeting is required. Refer to procedures in IRM 21.1.1.4, *Communication Skills*.
- (2) Employees are required to authenticate callers to ensure the person calling is the individual impacted by the data breach. See IRM 25.23.12.2, *Identity Theft Telephone General Guidance*, for required use of the Integrated Automation Technologies (IAT) Disclosure tool and the High-Risk Authorization (HRA) IAT tool to perform authentication; IRM 21.1.3.2.3, *Required Taxpayer Authentication*; and IRM 21.1.3.2.4, *Additional Taxpayer Authentication*.

- (3) If the caller is not the impacted individual, but claims to represent the individual, determine whether the individual provided a Power of Attorney (POA) in connection with the data breach. Do not recognize a representative when the POA on file identifies tax matters but doesn't specifically identify the data breach as a matter for which the POA has authority.
- (4) High-risk authentication per IRM 21.1.3.2.4, *Additional Taxpayer Authentication*, is also required. Ask the caller for the Breach Date and Breach Number as part of the authentication process. The Breach Date, if included in the letter, is located in the first paragraph of *Letter 4281C, IM Breach Notification Letter*. The Breach Number is located to the right and just above the Salutation (Dear Taxpayer).
- (5) In some situations, a caller may want to receive as much information as possible about the data breach but is not willing to provide his or her SSN/TIN. In these situations, the CSR may still answer general questions about the data breach and answer all the taxpayer's questions using the Frequently Asked Questions (FAQ), but a referral may not be made for any specific questions about the data breach. CSRs must be sensitive to the caller's tone and ensure they are given as much information as they are entitled to receive without the caller providing their TIN. See IRM 10.5.4.4.7.6, *Referrals to PGLD's Incident Management Office*, and IRM 10.5.4.4.7.8, *Updating History on Accounts Management Services (AMS) for Calls About IRS Data Breach Notification Letters*.
- (6) In some data breaches, impacted individuals receiving notices may be IRS employees. In these cases, follow guidance in IRM 21.1.3.8, *Inquiries from IRS Employees*.

10.5.4.4.7.3 (10-19-2017)

BMF Identity Check - AM IDT Toll-Free (App 161/162) Telephone Overview

- (1) Some of the impacted individuals may be business entities and letters sent may be to business related entities (sole proprietorships, corporations, LLCs, etc.). A caller may be required to be an owner of a small business or an officer of a corporation before employees are able to talk to him or her about the data breach. To ensure a caller is the appropriate individual that is allowed to receive information about the data breach, AM CSRs will need to conduct an identity check with the caller to determine if the individual is allowed to receive the information. See IRM 21.1.3.2.3, *Required Taxpayer Authentication*, for required use of the IAT Disclosure tool to perform authentication.
- (2) In addition to the authentication probes outlined in IRM 21.1.3.2.3, *Required Taxpayer Authentication*, ask the caller for the BMF entity to provide the following information:
 - The Breach Number, located to the right and just above the Salutation (Dear Taxpayer) on Letter 4281C, and
 - The Breach Date, located in the first paragraph of Letter 4281C.
- (3) If the caller is not able to, or unwilling to provide the EIN, tell the caller that a Referral may not be made for any specific questions about the data breach. See IRM 10.5.4.4.7.6, *Referrals to PGLD's Incident Management Office*, and IRM 10.5.4.4.7.8, *Updating History on Accounts Management Services (AMS) for Calls About IRS Data Breach Notification Letters*.

Note: It will not be necessary to access any tax account information on the BMF case to assist the caller. If at any time you feel the caller is not entitled to

receive general information, and the caller is insistent on receiving as much information as he or she can, be sure not to disclose any specific account information.

10.5.4.4.7.4
(09-02-2022)
Free Identity Protection/Identity Monitoring Service

- (1) The IRS is offering an identity protection/identity monitoring service at no cost to individuals potentially impacted by an IRS data breach if the risk assessment results in a likelihood of harm, specifically the potential for identity theft.

Note: The IRS assigns a unique enrollment code via *Letter 4281C, IM Breach Notification Letter*, to each individual potentially impacted by an IRS data breach if the risk assessment results in a likelihood of harm, specifically the potential for identity theft. The potentially impacted individuals must contact the identity protection/identity monitoring vendor within 90 days from the date of the letter to sign up for the free identity protection/identity monitoring service.

Note: A POA cannot sign up for the free identity protection/identity monitoring service on behalf of his or her client.

- (2) AM CSRs do not have access to the vendor's system; therefore, CSRs cannot assist the caller with the enrollment.

- (3) AM CSRs can assist with:

- Providing the toll-free number for the vendor. See Note below.
- Reviewing the online and telephone enrollment instructions included in Letter 4281C. See Note below.
- Informing the individual if he or she is having difficulty enrolling in the vendor's system, he or she has the option of speaking with a live agent by calling the vendor. Remind the individual he or she will need to have his or her unique enrollment code (assigned in Letter 4281C) available when contacting the vendor. See Note below.
- Ensuring the individual understands what he or she needs to do to monitor his or her credit report and other financial information. See Note below.

Note: See the *IRS Data Breach Frequently Asked Questions (FAQs)* on SERP for a list of frequently asked questions about Letter 4281C and general questions about IRS data breaches and the identity protection/identity monitoring vendors.

10.5.4.4.7.5
(10-22-2019)
Fraud Alerts

- (1) A fraud alert is a statement that a credit reporting agency adds to an individual's credit file at the individual's request. It alerts creditors that the individual may be a victim of fraud.
- (2) The fraud alert statement requires creditors to take certain steps to verify the individual's identity before establishing any new credit accounts in his or her name, issuing a new card on an existing account, or increasing the credit limit on an existing account.
- (3) All three credit reporting agencies (Equifax, Experian, and TransUnion) have fraud reporting services. The individual only needs to contact one of them. The agency initially contacted will notify the other two.
- (4) An individual can place a fraud alert on his or her credit file by contacting:

- Equifax at 800-525-6285 or www.equifax.com
- Experian at 888-397-3742 or www.experian.com
- TransUnion at 800-680-7289 or www.transunion.com

10.5.4.4.7.6
(10-07-2020)

**Referrals to PGLD's
Incident Management
Office**

- (1) If a caller states he or she received a letter from the IRS about a data breach but lost, misplaced the letter, etc., refer the caller to the IM office via Form 4442/e-4442, *Inquiry Referral*. See IRM 21.3.5.4.2, *How to Prepare a Referral*, for the required fields to be completed on Form 4442/e-4442.
- (2) If a caller states he or she attempted to redeem the enrollment code included in the data breach notification letter but was told the enrollment code is expired, invalid, or does not work, refer the caller to the IM office via Form 4442/e-4442, *Inquiry Referral*. See IRM 21.3.5.4.2, *How to Prepare a Referral*, for the required fields to be completed on Form 4442/e-4442.
- (3) If the caller is requesting additional information or details about the data breach, and is unsatisfied with the limited information you can provide and is insistent that he or she would like additional information, more than what was already provided, or wants to know why his or her spouse received a letter, and he or she didn't, or why his or her spouse received the free identity protection/identity monitoring offer, and he or she didn't, refer the caller to the IM office via Form 4442/e-4442, *Inquiry Referral*. See IRM 21.3.5.4.2, *How to Prepare a Referral*, for the required fields to be completed on Form 4442/e-4442.
- (4) In addition to the required fields as noted in IRM 21.3.5.4.2, if available, include the **Breach Date and Breach Number**, as shown on the caller's letter, in the **Referring To** field (Box #5) of Form 4442/e-4442, *Inquiry Referral*. The Breach Date, if included in the letter, is located in the first paragraph of *Letter 4281C, IM Breach Notification Letter*. The Breach Number is located to the right and just above the Salutation (Dear Taxpayer).
- (5) A brief narrative must be completed in the Taxpayer Inquiry/Proposed Resolution section (Part III, Section B) of Form 4442/e-4442, *Inquiry Referral*. Include in the Taxpayer Inquiry/Proposed Resolution section of the Form 4442/e-4442 the IRM reference (IRM 10.5.4.4.7.6) directing the referral, the reason you are making the referral, and a complete description of the caller's issue. Also document the response time frame provided to the caller and the fax number for PGLD/IM.
- (6) Inform the caller a referral has been completed in response to his or her inquiry. Tell the caller he or she will hear from us within 30 calendar days. See IRM 21.3.5.4, *Referral Procedures*.
- (7) Document AMS with the details of the Referral. See IRM 10.5.4.4.7.8, *Updating History on Accounts Management Services (AMS) for Calls About IRS Data Breach Notification Letters*. **EXCEPTION:** If the AMS or CIS system is down, then narratives and/or case notes will not be required.
- (8) All Forms 4442 will be collected by the Lead CSR at the beginning of each business day and faxed to the IM Office in Philadelphia. The IM EEFax number is listed on the *Form 4442 Referral Fax Numbers* list (Site: Philadelphia and Function: PGLD: Incident Management) located on the SERP Who/Where tab.

- (9) An analyst from PGLD/IM will contact the sender via secure email confirming receipt of the faxed Forms 4442. Once confirmation is made, the original Form 4442 can be destroyed. If no confirmation email is received within 48 hours from the fax date, re-fax the Form 4442 to PGLD/IM.
- 10.5.4.4.7.7
(09-02-2022)
Caller Indicates He or She is a Victim of Identity Theft as a Result of an IRS Data Breach
- (1) A caller who has already been notified of an IRS data breach via Letter 4281C may indicate he or she is already a victim of identity theft as a result of the IRS data breach and would like the IRS to assist him or her in dealing with the identity theft.
- (2) AM CSRs will:
- Apologize to the caller for any inconvenience.
 - Research the taxpayer’s TIN thoroughly to see if there is a tax related issue related to the ID theft as defined in IRM 25.23.2.3.5, *Identity Theft Research*.
 - If a tax related issue is involved, see IRM 25.23.12.4, *Tax-Related Identity Theft*.
 - Input an Identity Theft Tracking Indicator as directed in IRM 25.23.2.4.4, *Initial Allegation or Suspicion of Tax-Related identity Theft - IMF Identity Theft Indicators*.
- (3) If the taxpayer is threatening litigation or legal action because the IRS data breach resulted in identity theft, in addition to the above actions, prepare a Form 4442, *Inquiry Referral*, to alert the IM Office of the possible litigation or legal action. See the referral procedures in IRM 10.5.4.4.7.6, *Referrals to PGLD’s Incident Management Office*.
- 10.5.4.4.7.8
(09-02-2022)
Updating History on Accounts Management Services (AMS) for Calls About IRS Data Breach Notification Letters
- (1) The Privacy and Information Protection (PIP) toll-free number, 866-225-2009, is included in *Letter 4281C, IM Breach Notification Letter*, as well as the family of **obsoleted** letters (Letter 4281-A, Letter 4281-B, Letter 4281-E, Letter 4281-F, and Letter 4281-G) developed for the Get Transcript data breach. Individuals who call the PIP toll-free number are auto directed to the Identity Theft Product Line (Applications 161 and 162). AM CSRs working programs related to IM data breach notification letters are required to add an issue to identify the type of inquiry as well as leave a brief narrative of what was covered with the caller.
- Exception:** If the AMS or CIS system is down, then narratives and/or case notes will not be required.
- Note:** Although the SSN is not shown on Letter 4281C, employees will need to secure the caller’s SSN to update AMS. If the caller is unwilling to provide the employee with his or her SSN, it will not be possible to update AMS.
- 10.5.4.4.7.9
(10-19-2017)
Undelivered Letter 4281C
- (1) Undeliverable procedures must be followed. Refer to (3) of IRM 21.3.3.4.12.1.1, *Undelivered Mail Procedures for Accounts Management*, for research procedures for undeliverable mail.
- (2) If a new address is found, address an envelope with the new address and mail the undeliverable Letter 4281C to the new address.
- (3) If a new address is not found, treat Letter 4281C as classified waste.

Note: Because this process has to do with IRS data breaches, and not specifically tax related issues, do not contact a representative or a POA when referring to the Undeliverable procedures unless a POA specifically identifies the data breach as a matter for which the POA has authority.

10.5.4.4.8
(10-19-2017)
Retention and Disposition

- (1) IM will adhere to all document retention schedules in accordance with IRM 1.15, *Records and Information Management*. This applies to all materials in electronic or hard copy format created in response to an IRS data breach.

10.5.4.5
(10-19-2017)
IRS Data Breach Tracking Indicator - Objectives

- (1) The Incident Management Program tracks IRS data breaches to support the following objectives:
- a. Reduce taxpayer burden while addressing IRS data breaches.
 - b. Increase operational efficiency of the IRS by detecting and processing reported IRS data breaches as early and consistently as possible.

10.5.4.5.1
(03-02-2023)
IRS Data Breach Tracking Indicator - Development and Implementation

- (1) PGLD developed an IRS data breach tracking indicator to centrally track IRS data breaches.
- (2) The IRS data breach tracking indicator was implemented by PGLD to identify individuals whose PII was lost, stolen, or disclosed as a result of an IRS data breach and the data breach risk assessment results in a likelihood of harm to the potentially impacted individuals.
- (3) The IRS data breach tracking indicator is input as a Transaction Code (TC) 971 with Action Code (AC) 505. The TC 971 AC 505 is displayed on the Integrated Data Retrieval System (IDRS) on the entity portion of each impacted individual's account (CC ENMOD and CC IMFOLE).

10.5.4.5.1.1
(10-07-2020)
Applying the IRS Data Breach Tracking Indicator to IRS Data Breaches

- (1) The TC 971 AC 505 is an **IRS Data Breach Tracking Indicator - not an identity theft indicator**.
- (2) The TC 971 AC 505:
- a. **Will not** block, or prevent, online system access.
 - b. **Will not** stop registration for online services, including registration for Get Transcript or an Identity Protection Personal Identification Number (IP PIN).
 - c. **Will not** stop paper requests for a transcript (Form 4506/T).
- (3) PGLD/IM inputs a TC 971 AC 505 on the entity portion of an individual's account (as long as the entity is established on the Master File) when all the following occur:
- a. An individual's IRS-held PII was lost, stolen, or disclosed.
 - b. The data breach risk assessment results in a likelihood of harm to the potentially impacted individuals.
 - c. The IRS notifies the individual of the data breach via Letter 4281C, *IM Breach Notification Letter*, or similar letter in some circumstances (such as letters developed for the Get Transcript data breach).

Example: Case files containing PII were lost while being shipped from one location to another. Since the data breach risk assessment resulted in a likelihood of harm, IM will send data breach notification letters to the potentially impacted individuals.

- (4) A TC 971 AC 505 will only be input on the accounts of individuals who are sent Letter 4281C because of an *intentional unauthorized access or disclosure* if they are offered identity protections *such as* identity protection/identity monitoring services or IP PIN in the letter. If they are only advised of their rights under IRC 7431, then no TC 971 AC 505 will be input.
- (5) Input of TC 971 AC 505 is limited and reserved for use by PGLD/IM employees; however, this indicator is visible and available for reference on the entity portion (CC ENMOD or CC IMFOLE) of an individual's account. See Exhibit 10.5.4-2, *TC 971 AC 505 — IRS Data Breach Indicator*, for more information about this indicator.

Note: At the request of PGLD/IM, for large scale data breaches, the TC 971 AC 505 may be uploaded directly to CC IMFOLE by Return Integrity and Compliance Services (RICS).

- (6) PGLD/IM inputs TC 971 AC 505 on an account regardless of the existence of any identity theft indicator codes that may be present on the account.
- (7) There can be multiple IRS data breach indicators input/present on an individual's account. Each TC 971 AC 505 represents a different IRS data breach.
- (8) In some instances, it may be necessary for PGLD/IM personnel to manually reverse the TC 971 AC 505. Although input of the TC 972 AC 505 is limited and reserved for use by PGLD/IM employees, Exhibit 10.5.4-3, *TC 972 AC 505 — Reversal of TC 971 AC 505*, is included in this IRM to explain the values in the TC 972 AC 505 Miscellaneous field.

This Page Intentionally Left Blank

Exhibit 10.5.4-1 (03-02-2023)

Glossary of Incident Management Terms, Definitions, and Acronyms

TERM	DEFINITION
Access	The authority granted to employees and contractors that provide opportunity to physically come into contact with (including, but not limited to reading, transporting, and/or transcribing/interpreting) Sensitive But Unclassified (SBU) data in the performance of official duties; entering an IRS facility without escort; and/or to login to IRS systems with approved credentials.
Accounts Management (AM) Customer Service Representatives (CSRs)	AM CSRs assist individuals impacted by IRS data breaches by answering general data breach related inquiries or preparing a Form 4442, <i>Inquiry Referral</i> , if the caller requests specific information about the data breach that the AM CSR is unable to answer. AM CSRs also provide assistance to individuals impacted by identity theft or individuals who could become victims of identity theft in the future due to a data loss such as a lost or stolen purse/wallet, questionable credit card activity, etc. This assistance is provided by AM CSRs even if the individual has not experienced any problems with, or received communications from, the IRS.
Audience	The employees responsible for taking action or who require knowledge about the program, process or activity.
Breach Response Team (BRT)	The BRT is the group of individuals that will respond to a high-risk data breach or any data breach that constitutes a major incident as defined in OMB guidance. See Document 13347, <i>Data Breach Response Playbook</i> , for additional information about the BRT.
Bring Your Own Device (BYOD)	Bring Your Own Device is a concept that allows employees to use their personally owned technology devices to stay connected to, access data from, or complete tasks for their organizations. At a minimum, BYOD programs allow users to access employer-provided services and/or data on their personal tablets/eReaders, smartphones, and other devices.

Exhibit 10.5.4-1 (Cont. 1) (03-02-2023)

Glossary of Incident Management Terms, Definitions, and Acronyms

TERM	DEFINITION
Business Unit (BU) Data Owner	The BU who has responsibility for the data/information and is therefore responsible for containment and mitigation of the data breach, e.g., if a Power of Attorney (POA) tells an SBSE Revenue Officer (RO) she received IVES transcripts she did not request, the reporting employee is the RO, but W&I is the data owner and carries the responsibility for mitigation and containment. Note that Data Owner is synonymous with Information Owner . Per IRM 10.8.2.2.1.6, <i>Information Owner</i> , The Information Owner is an IRS official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. At the IRS, the Information Owner is the Business and Functional Unit Owner.
Computer Security Incident Response Center (CSIRC)	Responsible for monitoring the IRS network 24 hours a day year-round for cyberattacks and computer vulnerabilities and for various security incidents such as the theft of a laptop computer.
Data Breach	OMB M-17-12 defines a data breach as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person, other than an authorized user accesses or potentially accesses personally identifiable information, or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose. Note: See also the definition of "Incident."
Data Breach Incident	An incident involving a loss, theft, or inadvertent unauthorized disclosure of SBU data, including PII and tax information. A few common examples include: a laptop or portable storage device storing PII is lost or stolen; an email containing PII is inadvertently sent to the wrong person; or a box of documents with PII is lost or stolen during shipping.
Data Breach Management	The process of managing incidents involving a loss, theft, or inadvertent unauthorized disclosure of SBU data, including PII and tax information.
Data Breach Notification	The process of notifying potentially impacted individuals following the evaluation of an incident involving a loss, theft, or inadvertent unauthorized disclosure of SBU data, including PII and tax information, which results in a likelihood of harm to these individuals.

Exhibit 10.5.4-1 (Cont. 2) (03-02-2023)

Glossary of Incident Management Terms, Definitions, and Acronyms

TERM	DEFINITION
Data Breach Risk Assessment	A risk assessment conducted on an incident involving a loss, theft, or inadvertent unauthorized disclosure of SBU data, including PII and tax information. The risk assessment includes factors that must be considered, specifically the context of the data breach and the data that was disclosed. Example: An IRS employee in the field loses a taxpayer case file. The case file contained PII data such as name, address, social security number, and other tax data. It is not known if the loss of the PII data will lead to identity theft. The IRS conducts a risk assessment and examines key factors to determine if notification must be given to the potentially impacted individual.
Disclosure	Making known to any person, in any manner, a return or return information. IRC 6103 governs the rules for how, when, to whom, and what federal tax information can or cannot be disclosed. See IRM 11.3.1, <i>Disclosure of Official Information, Introduction to Disclosure</i> .
Enterprise Electronic Fax (EEFax)	Enterprise Electronic Fax is the Servicewide standard system for secure faxing. It allows you to send and receive electronic documents directly from your computer. Incoming faxes appear as Adobe Acrobat pdf files in your group EEFax from no reply@efax.gov.
Erroneous Taxpayer Correspondence (ETC)	Correspondence is erroneous when it has been sent to the wrong address or addressee and it involves SBU data, including PII and tax information. Erroneous taxpayer correspondence can also be notices, letters, transcripts, faxes, or other electronic/digital documents sent with mixed entity information such as correct taxpayer information is on page one, but unrelated taxpayer information is on page two; two letters for different taxpayers in the same envelope; the attachment in the correspondence is for a different taxpayer, etc.
Federal Information Processing Standards (FIPS)	A set of standards that describe document processing, encryption algorithms and other information technology standards for use within non-military government agencies and by government contractors and vendors who work with the agencies.
Federal Information Processing Standards (FIPS) Publications	Publications issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Reform Act of 1996 (Public Law 104-106) and the Federal Information Security Management Act of 2002 (Public Law 107-347).

Exhibit 10.5.4-1 (Cont. 3) (03-02-2023)**Glossary of Incident Management Terms, Definitions, and Acronyms**

TERM	DEFINITION
Federal Tax Information (FTI)	Any return or return information received from the IRS or secondary source, such as SSA etc. FTI includes any information created by the recipient that is derived from return or return information. (IRC 6103, Confidentiality and disclosure of returns and return information.) See IRM 10.5.1, <i>Privacy and Information Protection, Privacy Policy</i> , for additional information.
Federal Trade Commission (FTC)	An independent agency of the United States government, established in 1914 by the Federal Trade Commission Act, with the principal mission of promoting “consumer protection” and the elimination and prevention of what regulators perceive to be “anti-competitive” business practices.

Exhibit 10.5.4-1 (Cont. 4) (03-02-2023)

Glossary of Incident Management Terms, Definitions, and Acronyms

TERM	DEFINITION
<p>Form 14164, Personally Identifiable Information (PII) Analysis</p>	<p>Employees report data breaches involving erroneous taxpayer correspondence involving the disclosure of SBU data, including PII and tax information, i.e., a notice, letter, or transcript, which was mailed, emailed, faxed, EEFaxed, or generated or transmitted via IVES, RAIVS, TDS, SDT, or other electronic transmission, to the wrong address or addressee; or inadvertent unauthorized disclosures of SBU data, including PII and tax information, such as verbal disclosures, or emails sent to the wrong person or not properly encrypted; or the loss, theft, or unauthorized destruction of documents containing SBU data, including PII and tax information, such as hardcopy records, documents, or case files, packages lost or stolen during UPS or FedEx shipment, or lost or stolen remittances; or electronic disclosures of SBU data, including PII and tax information, in IRMs, Training Materials, PowerPoints, IRS Source, SharePoint, etc., or on external systems/sites such as WhatsApp, GitHub, etc., via PGLD’s e-Trak online breach reporting form (PII Breach Reporting Form). The online breach reporting form is a web-based online reporting form fillable only through e-Trak, a web interface for case tracking. The Personally Identifiable Information (PII) Analysis form is auto-populated through e-Trak based on the information the reporting employee enters on the e-Trak online breach reporting form. Form 14164 is generated for informational purposes to provide reporting employees with a summary of their responses from the e-Trak online breach reporting form for their records. If the reporting employee indicated there was PII involved in the data breach on the e-Trak online breach reporting form, e-Trak generates a Form 14164, PII Analysis, and includes it, and Excel spreadsheets, in an email sent to the employee. The email requests the employee identify the impacted individuals and/or businesses on the spreadsheets attached to the email and to return the completed spreadsheets within two business days to the *PII mailbox. Note: Form 14164 is viewable from the Publishing Catalog, but it is not fillable.</p>

Exhibit 10.5.4-1 (Cont. 5) (03-02-2023)

Glossary of Incident Management Terms, Definitions, and Acronyms

TERM	DEFINITION
Form 14164-A, Personally Identifiable Information (PII) Breach Reporting	Employees report data breaches involving erroneous taxpayer correspondence involving the disclosure of SBU data, including PII and tax information, i.e., a notice, letter, or transcript, which was mailed, emailed, faxed, EEFaxed, or generated or transmitted via IVES, RAIVS, TDS, SDT, or other electronic transmission, to the wrong address or addressee; or inadvertent unauthorized disclosures of SBU data, including PII and tax information, such as verbal disclosures, or emails sent to the wrong person or not properly encrypted; or the loss, theft, or unauthorized destruction of documents containing SBU data, including PII and tax information, such as hardcopy records, documents, or case files, packages lost or stolen during UPS or FedEx shipment, or lost or stolen remittances; or electronic disclosures of SBU data, including PII and tax information, in IRMs, Training Materials, PowerPoints, IRS Source, SharePoint, etc., or on external systems/sites such as WhatsApp, GitHub, etc., via PGLD's e-Trak online breach reporting form (PII Breach Reporting Form). The online breach reporting form is a web-based online reporting form fillable only through e-Trak, a web interface for case tracking. Note: A representation of the PII Breach Reporting Form is viewable from the Publishing Catalog, but it is not fillable. It is only accessible/fillable on e-Trak. The fillable version on e-Trak contains drop-down selections to aid in completion of the form.
Fraud Alert	A fraud alert is a statement that a credit reporting agency adds to an individual's credit file at the individual's request. It alerts creditors that the individual may be a victim of fraud. This statement requires creditors to take certain steps to verify the individual's identity before establishing any new credit accounts in his or her name, issuing a new card on an existing account, or increasing the credit limit on an existing account.
Harm/Risk of Harm	Includes any of the following effects of a breach of confidentiality, integrity, availability, or fiduciary responsibility:
	a) Potential for blackmail;
	b) Disclosure of private facts;
	c) Mental pain and emotional distress;
	d) Potential for secondary uses of the information that could result in fear or uncertainty, or unwarranted exposure leading to humiliation or loss of self-esteem;
	e) Identity theft; or
f) Financial loss.	

Exhibit 10.5.4-1 (Cont. 6) (03-02-2023)

Glossary of Incident Management Terms, Definitions, and Acronyms

TERM	DEFINITION
Identity Theft	Use of an individual's personal information, without the individual's permission, to commit fraud or other crimes.
Incident	OMB M-17-12 defines an Incident as an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. An incident is classified as an incident if it involves SBU information but doesn't involve PII. Often, an occurrence may be first identified as an incident , but later identified as a data breach once it is determined that the incident involves PII, as is often the case with a lost or stolen laptop or electronic storage device. Note: See also the definition of "Data Breach."
Incident Management (IM)	Incident Management (IM) refers to the Office within Privacy, Governmental Liaison and Disclosure responsible for the process of managing incidents involving a loss, theft, or inadvertent unauthorized disclosure of SBU data, including PII and tax information, by the IRS.
Incorrect Correspondence	A notice or letter (received traditionally or digitally) containing one or more of the following issues: misspellings or bad grammar; incorrect IRS phone numbers; incorrect QR codes or URL Links; incorrect, missing, or unreadable text; or incorrect account information.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency.
Loss	Any event where an item is misplaced and/or neither the official owner nor the intended recipient has possession of the item in the expected time frame. A loss may involve an IRS-owned physical asset such as a laptop, blackberry, cell phone, and/or other portable media, or electronic or hard copy data that may contain Sensitive But Unclassified (SBU) data, including Personally Identifiable Information (PII) and tax information, such as paper or electronic taxpayer records, personnel records, or other identifying data, or a combination of a physical asset and electronic and/or hard copy data. A loss involving PII is known as a Data Breach .

Exhibit 10.5.4-1 (Cont. 7) (03-02-2023)

Glossary of Incident Management Terms, Definitions, and Acronyms

TERM	DEFINITION
Major Incident	OMB M-23-03, <i>Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements</i> , defines a <i>major incident</i> as any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. A <i>data breach</i> (see the definition of “data breach” above) constitutes a <i>major incident</i> when it involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. An unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to 100,000 or more individuals’ PII constitutes a <i>major incident</i> .
National Archives and Records Administration (NARA)	NARA is an independent agency of the U.S. Government charged with the preservation and documentation of government and historical records. NARA establishes policies and procedures for managing U.S. Government records and assists federal agencies in administering records management programs and related activities.
National Institute of Standards and Technology (NIST)	A non-regulatory federal agency within the U.S. Department of Commerce that develops and promotes measurement, standards, and technology.
The Office of Management and Budget (OMB)	OMB assists the President in overseeing the preparation of the Federal budget and evaluates the effectiveness of agency programs, policies, and procedures, and works to make sure that agency reports, rules, testimony, and proposed legislation are consistent with the President’s Budget and with Administration policies. In addition, OMB oversees and coordinates the Administration’s regulatory, procurement, financial management, information technology, and information management policies.
Personally Identifiable Information (PII)	The term PII refers to information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual. See OMB M-17-12, at https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2017/m-17-12_0.pdf and the PGLD webpage, <i>Personally Identifiable Information</i> for additional information.

Exhibit 10.5.4-1 (Cont. 8) (03-02-2023)

Glossary of Incident Management Terms, Definitions, and Acronyms

TERM	DEFINITION
Phishing	Phishing is a scam where Internet fraudsters send email messages to trick unsuspecting victims into revealing personal and financial information that can be used to steal the victim's identity. See IRM 21.1.3.23, <i>Scams (Phishing) and Fraudulent Schemes</i> .
PII Working Group (PIIWG)	A decision-making body consisting of senior management and technical experts from all key business and functional unit stakeholders with expertise in information technology, legal requirements, privacy, law enforcement and information security.
Policy Owner	The IRS organization or the title of the executive (position only) responsible for the program.
Potentially Impacted Individual	Individuals, as defined by the Privacy Act of 1974, potentially impacted by occurrences of IRS data losses, thefts, and inadvertent unauthorized disclosures involving SBU data, including PII and tax information, are known as "Potentially Impacted Individuals". Consistent with OMB directives, the IRS notifies potentially impacted individuals when a data breach involves the loss, theft, or inadvertent unauthorized disclosure of PII, and the result of the risk assessment indicates there is a potential risk that the compromised data may be used by someone other than the owner of the information to commit a crime or fraud.
Program Owner	The office which has primary responsibility for establishing the policy, process, and procedures to implement and manage the IRS program. Directors within this office are responsible for developing and publishing IRM procedures. The program owner is the IRM owner for the program.
Records	Includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them. (44 USC 3301).
Records and Information Management	In keeping with the Federal Records Act of 1950, as amended, and pursuant to 44 USC 3102, the IRS established a records management program - renamed Records and Information Management (RIM) Program - to ensure the economical and efficient management of its records in the creation, maintenance, retrieval, preservation, and disposition of all records.

Exhibit 10.5.4-1 (Cont. 9) (03-02-2023)

Glossary of Incident Management Terms, Definitions, and Acronyms

TERM	DEFINITION
Reporting Employee	The reporting employee is the employee who identifies/ recognizes a data breach and reports the data breach as required. The reporting employee is responsible for reporting all pertinent information relative to the data breach.
Risk	The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
Risk Assessment	The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security and privacy controls that would mitigate this impact.
Safeguard	Any action, device, procedure, technique, or other measure that reduces a system's vulnerability to a threat.
Safeguarding Personally Identifiable Information Data Extracts (SPIIDE)	A Data Loss Prevention (DLP) tool within the IRS Cybersecurity toolkit. DLP is technology that scans unencrypted, outbound transmissions to advance data protection and reduce inadvertent disclosures.
Sensitive But Unclassified (SBU) Data	Any information which if lost, stolen, misused, or accessed or altered without proper authorization, may adversely affect the national interest or the conduct of federal programs (including IRS operations), or the privacy to which individuals are entitled under the Privacy Act (5 USC 552).
Sensitive But Unclassified (SBU). See TD P 15-71, Treasury Security Manual, Chapter III Section 24, Sensitive But Unclassified Information	The term "Sensitive But Unclassified" originated with the Computer Security Act of 1987. It defined SBU as "any information the loss, misuse, or unauthorized access to, or modification of, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under 5 USC 552a (the Privacy Act), but has not been specifically authorized under criteria established by an Executive Order or an act of Congress to be kept classified in the interest of national defense or foreign policy." Examples of such sensitive information include personal financial information and information that discloses law enforcement investigative methods. Other particular classes of information may have additional statutory limits on disclosure that require that information to also be treated as sensitive. Examples include tax information, which is protected by IRC 6103 (26 USC 6103) and advanced procurement information, protected by the Procurement Integrity Act (41 USC 423).

Exhibit 10.5.4-1 (Cont. 10) (03-02-2023)

Glossary of Incident Management Terms, Definitions, and Acronyms

TERM	DEFINITION
Situational Awareness Management Center (SAMC)	SAMC is tasked with promptly reporting all physical security incidents and/or threats.
Tax Information	The term “tax information” refers to a taxpayer’s return and return information protected from unauthorized disclosure under IRC 6103. The law defines return information as any information the IRS has about a tax return or liability determination. Tax information in IRS business processes comes under many names, such as Federal Tax Information (FTI), IRC 6103 protected information, taxpayer data, taxpayer information, tax return information, return information, case information, SBU data, and PII. See IRM 10.5.1, <i>Privacy and Information Protection, Privacy Policy</i> , for additional information.
TCSIRC	Treasury Computer Security Incident Response Center
TSSSOC (formerly GSOC)	Treasury Shared Services Security Operations Center (formerly Treasury Government Security Operations Center)
Theft	An asset, electronic or hardcopy, thought or known to have been taken without permission from the individual who is responsible for the asset.
Third-Party Data Owner	Data owner external to the IRS.
Third-Party Data Breach	An event that results from the unauthorized use or loss of SBU data (including PII and tax information) that does not involve IRS systems, applications, or online services. Third-party data breaches can be reported to the IRS by external sources, such as practitioners, software developers, state and local agencies, or others.
Treasury Inspector General for Tax Administration (TIGTA)	Provides oversight of the Department of the Treasury matters involving IRS activities, the IRS Oversight Board and the IRS Office of Chief Counsel.
Unauthorized Access	The willful unauthorized access and/or inspection of tax returns and return information.
Unauthorized Disclosure	An unauthorized and unlawful release of information to an individual who is not authorized to receive the information.

Exhibit 10.5.4-1 (Cont. 11) (03-02-2023)**Glossary of Incident Management Terms, Definitions, and Acronyms**

TERM	DEFINITION
Unreasonable Delay	A delay in notification following the discovery of a data breach beyond that which is necessary to determine the scope of the data breach while considering the needs of law enforcement and national security, and, if applicable, to restore the reasonable integrity of the computerized data system compromised. This means if a data breach is discovered and all the information necessary to determine the scope of the data breach is gathered within 30 days, it is unreasonable to wait until the 45th day to notify the individuals whose information was breached.
US-CERT	United States Computer Emergency Readiness Team

Exhibit 10.5.4-2 (06-25-2013)

TC 971 AC 505 — IRS Data Breach Indicator

Important: Input of Action Code 505 is limited and reserved for use by the Office of Privacy, Governmental Liaison and Disclosure (PGLD) personnel.

TC 971 AC 505 is displayed on IDRS command code ENMOD and consists of the following data elements:

TRANS-DT	SECONDARY-DT	MISC
TC 971 AC 505 input date	Date the IRS data breach occurred.	The Breach Tracking Number (number assigned to the breach). This number begins with two alphas ("IR", "CR", or "PR") and is followed by 11 numeric digits. For example: IR20100211034

Exhibit 10.5.4-3 (12-10-2010)**TC 972 AC 505 — Reversal of TC 971 AC 505**

Important: Input of Action Code 505 is limited and reserved for use by the Office of Privacy, Governmental Liaison and Disclosure (PGLD) personnel.

The miscellaneous field for TC 972 AC 505 reflects the reason for the reversal of TC 971 AC 505. See the following chart for reasons and values for the MISC field:

Reason	Description	Value
Keying or Internal Error	The 971 was due to a typographical mistake or another internal mistake.	IRSERR
Internally Identified Negative Impact	The 971 is causing a negative impact on another internal process or system and must be reversed to discontinue the negative impact.	IRSADM
Other	The reason for the 971 reversal does not meet any of the above reason descriptions.	OTHER