MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.5.8

FEBRUARY 20, 2018

EFFECTIVE DATE

(02-20-2018)

PURPOSE

(1) This transmits the revised IRM 10.5.8, *Privacy and Information Protection, Sensitive But Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments*.

MATERIAL CHANGES

(1) Reviewed and updated website addresses throughout the IRM and made other editorial changes to IRM 10.5.8.3.4.1 and IRM 10.5.8.3.6.1.

(2) IRM 10.5.8.1 - Revised the title to *Program, Scope and Objectives*, to properly reflect the information communicated in this subsection. Information from prior subsections 10.5.8.1, 10.5.8.1.1, and 10.5.8.1.3 was incorporated into this new subsection. Restructured previous content to conform to the new internal and management control standards under the following titles:

a. IRM 10.5.8.1.1, *Background* - Incorporates information from prior Background section of the 9-28-2015 revision Manual Transmittal.

b. IRM 10.5.8.1.4, *Terms, Definitions and Acronyms* - Incorporates information from prior subsection 10.5.8.1 as well as a reference to IRM Exhibit 10.5.8-1.

(3) The following table reflects additional content migration from the 9-28-2015 revision of IRM 10.5.8 to the current revision:

New Subsection Number	Title	9-28-2015 Revision Subsection Number
10.5.8.1.2	Authorities	10.5.8.1.2
10.5.8.1.2.1	Privacy Authorities	10.5.8.1.2.1
10.5.8.1.2.2	IT Security Authorities	10.5.8.1.2.2
10.5.8.1.3	Roles and Responsibilities	10.5.8.2
10.5.8.1.3.1	Privacy Compliance and Assurance (PCA)	10.5.8.2.1
10.5.8.1.3.1.1	Approval Authority for PCA	10.5.8.2.1.1
10.5.8.1.3.2	Information System Owner (SO)	10.5.8.2.2
10.5.8.1.3.3	Authorizing Official (AO)	10.5.8.2.3
10.5.8.1.3.4	Information Owner (IO)	10.5.8.2.4
10.5.8.2	Risk Acceptance and Risk-Based Decisions	10.5.8.1.4

EFFECT ON OTHER DOCUMENTS

IRM 10.5.8 dated September 28, 2015 is superseded.

AUDIENCE

IRM 10.5.8 shall be distributed to all personnel responsible to preserve and enhance public confidence by advocating for the protection and proper use of identity information. This policy applies to all employees, contractors, and vendors of the IRS whose job function requires the use of SBU data in any form and any subsystem including, but not limited to: engineering, pre-production, planned modification, testing, maintaining software, research, emergency issue resolution, and auditing.

Frances Kleckley
Director, Privacy Policy and Compliance (PPC)

10.5.8

Sensitive But Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments

Table of Contents

#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#

Exhibits

10.5.8.1
(02-20-2018)
Program Scope and Objectives

(1) This IRM establishes privacy and Information Technology (IT) security controls for the use and protection of Sensitive But Unclassified (SBU) data.

Note: As in IRM 10.8.1, the requirements within this policy are organized to follow the order in which security controls are presented within National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision (Rev) 4. In an effort to reference the origin of a security requirement (NIST, Treasury, etc.), a requirement may have its origin referenced in parenthesis at the end of the requirement; such as (NIST AC-1) or (TD P 85-01 S-PM.1).

(2) This IRM further establishes the minimum baseline privacy and IT security policy and requirements for all non-production environments using IRS SBU data in order to:

a. Protect against attacks that exploit IRS assets.
b. Prevent unauthorized access.
c. Enable IRS IT computing environments that meet the security requirements of this policy and support the business needs of the organization.

(3) This IRM also covers the use and protection of SBU data in a non-production IRS or vendor environment (e.g., testing, development, Priority 1/Priority 2 (P1/P2) ticket incidents requiring a vendor's environment for resolution, planned non-production vendor environment).

(4) This IRM also addresses the approval, acquisition, handling, protection, and disposition of SBU data in non-production environments.

(5) The provisions in this IRM apply to:

a. All offices and business, operating, and functional units within the IRS.
b. Individuals and organizations having contractual arrangements with the IRS, including employees, contractors, vendors, and outsourcing providers, which use or operate information systems that store, process, or transmit IRS Information or connect to an IRS network or system.

   Note: This IRM covers all systems operated by and on behalf of the IRS no matter what stage of the IT lifecycle they are in (i.e., production, pre-production, and post-production systems).

c. All IRS information and information systems. For information systems that store, process, or transmit classified information, please refer to IRM 10.9.1, *National Security Information*, for additional procedures for protecting classified information.

(6) It is acceptable to configure settings to be more restrictive than those defined in this IRM.

(7) For more information regarding SBU, refer to IRM 10.5.1, *Privacy and Information Protection, Privacy Policy*, and IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance*.

10.5.8.1.1
(02-20-2018)
Background

(1) Federal Information Processing Standards (FIPS) 200 mandates the use of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 as an initial set of baseline security controls for the creation of agency IT security policy. Additionally, the IRS is bound by statute, regulation, and policy to protect the SBU data in its possession. This IRM describes how Information Owners and data users shall ensure that the risk to the confidentiality of SBU data is appropriately mitigated when used in non-production environments.

(2) IRM 10.5.8 is part of the Security, Privacy and Assurance policy family, IRM Part 10 series for IRS Privacy and Information Protection.

10.5.8.1.2
(02-20-2018)
Authorities

(1) This IRM addresses privacy and IT security controls per NIST guidance and SBU data protection per Federal regulations and mandates.

(2) The following subsections provide further details on privacy and IT authorities.

10.5.8.1.2.1
(02-20-2018)
Privacy Authorities

(1) IRC §6103 – Confidentiality and Disclosure of Returns and Return Information.

(2) Privacy Act of 1974 (see IRM 11.3.14).

(3) IRS Privacy Principles: Among the most basic of taxpayer and employee expectations is that the Internal Revenue Service will protect the privacy of personal information - including financial and employment information - regardless of medium, including paper. The Service is dedicated to meeting these expectations. All Service employees and contractors are required to act in a way that reflects a commitment to deal with individuals fairly, honestly, and respectfully and to protect their right to privacy at all times. Protecting taxpayer privacy and safeguarding confidential taxpayer information is a matter of public trust. To maintain the trust of both taxpayers and its employees, the Service will be guided by the following privacy principles:

1. Accountability
2. Purpose Limitation
3. Minimizing Collection, Use, Retention, and Disclosure
4. Openness and Consent
5. Strict Confidentiality
6. Security
7. Data Quality
8. Verification and Notification
9. Access, Correction, and Redress
10. Privacy Awareness and Training

Note: Descriptions of these principles can be found at: *https://portal.ds.irsnet.gov/sites/vl003/Lists/PrivacyPolicyPrivacyControls/DispItemForm.aspx?ID=23*

(4) NIST Special Publication 800-53, Rev. 4, Appendix J: Privacy Control Catalog.

- Data Minimization and Retention Family (DM): Helps organizations implement data minimization requirements to collect, use, and retain only the Personally Identifiable Information (PII) that is relevant and necessary for the purpose for which it was originally collected.

- DM-3 – Minimization of PII used in testing, training, and research: Requires organizations to develop policies and procedures to minimize use of PII for these purposes and to implement controls to protect PII when use is necessary.

(5) Office of Management and Budget (OMB) Memorandum M-07-16: Safeguarding Against and Responding to the Breach of Personally Identifiable Information.

(6) For a comprehensive list of privacy-related authorities, please refer to Exhibit 10.5.8-2, *References*.

10.5.8.1.2.2
(02-20-2018)
IT Security Authorities

(1) Per Federal Information Processing Standards (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*:

Policies and procedures play an important role in the effective implementation of enterprise-wide information security programs within the federal government and the success of the resulting security measures employed to protect federal information and information systems. Thus, organizations must develop and promulgate formal, documented policies and procedures governing the minimum security requirements set forth in this standard and must ensure their effective implementation.

a. Special Publications (SPs) are developed and issued by NIST as recommendations and guidance documents. For other than national security programs and systems, federal agencies must follow those NIST Special Publications mandated in a Federal Information Processing Standard (FIPS). FIPS 200 mandates the use of Special Publication 800-53, as amended. In addition, OMB policies (including OMB Reporting Instructions for Federal Information Security Management Act of 2002 (FISMA) and Agency Privacy Management) state that for other than national security programs and systems, federal agencies must follow certain specific NIST Special Publications.
b. While federal agencies are required to follow certain specific NIST Special Publications in accordance with OMB policy, agencies have flexibility in how to apply the guidance. Federal agencies apply the security concepts and principles articulated in the NIST Special Publications in accordance with and in the context of the agency's missions, business functions, and environment of operation. Consequently, the application of NIST guidance by federal agencies can result in different security solutions that are equally acceptable, compliant with the guidance, and meet the OMB definition of adequate security for federal information systems.

(2) IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance*, establishes the security program and the policy framework for the IRS.

10.5.8.1.3
(02-20-2018)
Roles and Responsibilities

(1) IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities*, defines IRS-wide roles and responsibilities related to IRS information and computer security, and is the authoritative source for such information.

10.5.8.1.3.1
(02-20-2018)
Privacy Compliance and Assurance (PCA)

(1) PCA, as the owner and manager of the SBU Data Usage and Protection program for IRS, is responsible for:

a. Implementing this IRM, including developing procedures, establishing compliance requirements, and approving SBU Data Usage requests.
b. Establishing Sensitive Data Usage and Protection policy, in collaboration with IT security and Privacy Policy.

(2) PCA's Associate Director may delegate certain assurance activities within the SBU Data Usage and Protection procedures to the Information Owner (IO).

10.5.8.1.3.1.1
(02-20-2018)
Approval Authority for PCA

(1) The Associate Director shall have approval authority for PCA. The Associate Director may delegate this authority to the first-line manager over the SBU Data program.

10.5.8.1.3.2
(02-20-2018)
Information System Owner (SO)

(1) The Information System Owner is the official responsible for the overall procurement, development, integration, modification, and operation and maintenance of the information system. Refer to IRM 10.8.2 for more detail about the Information System Owner.

10.5.8.1.3.3
(02-20-2018)
Authorizing Official (AO)

(1) The Authorizing Official (AO) of the environment (e.g., system or application) that uses the requested SBU data shall be responsible for protecting the data throughout the time of its use and final disposition.

a. The AO shall ensure that the documentation of access privileges of personnel authorized to use SBU data is maintained and actively reviewed to be accurate at all times.
b. Refer to the Information Owner section in this IRM for additional guidance regarding the specific responsibilities of the sending environment AOs when a single IO cannot be determined.
c. If receiving environment gets a new AO or the new sending environment AO functions as the IO, the new AO shall have up to 30 calendar days to re-sign the SBU Data Use Questionnaire, Request, and Recertification forms that the previous AO had signed.

(2) Refer to IRM 10.8.2, *IT Security Roles and Responsibilities*, for additional information regarding the roles and responsibilities of the Information Owner and the Authorizing Official.

10.5.8.1.3.4
(02-20-2018)
Information Owner (IO)

(1) The Information Owner (IO) of the production environment that sends the SBU data to a non-production environment is ultimately responsible for the protection of SBU data in accordance with this policy.

a. Where the sending environment contains data from multiple sources or has unclear provenance, the sending environment IO shall have all of the responsibilities contained in this section.
b. Where the identity of the IO of the sending environment is unclear, the sending environment AO shall have the authority to perform these IO responsibilities.
c. In determining whether or not to permit access to the requested SBU data, the IO shall analyze the non-production environment's security controls.
d. The IO shall assess the risks presented by the receiving environment AO.

e. When permitting or denying access to SBU data, the IO accepts or rejects risk.
f. The receiving environment AO and the IO shall work closely with PCA to mitigate any risk noted as unacceptable.
g. If the environment gets a new IO, the new IO shall have up to 30 calendar days to re-sign the SBU Data Use Questionnaire, Request, and Recertification forms that the previous IO had signed.

(2) Refer to IRM 10.8.2, *IT Security Roles and Responsibilities*, for additional information regarding the roles and responsibilities of the Information Owner and the Authorizing Official.

10.5.8.1.4
(02-20-2018)
Terms, Definitions and Acronyms

(1) For the purposes of this IRM, SBU is any data that the IRS considers sensitive from a confidentiality or other risk point of view. SBU data includes:

- Federal Tax Information (FTI)
- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Certain procurement information
- System vulnerabilities
- Case selection methodologies
- Systems information
- Enforcement procedures
- Investigation information
- Proprietary processes or algorithms used in investigative work or tax processing

Note: Live data, which is defined as production data in use (production, testing, development), often contains SBU.

(2) See Exhibit 10.5.8-1, *Glossary and Acronyms*, for full details on the terms and acronyms used in this IRM and their respective definitions.

10.5.8.2
(02-20-2018)
Risk Acceptance and Risk-Based Decisions

(1) Using this SBU data policy and Privacy Compliance and Assurance's (PCA's) procedures is equivalent to making a risk-based decision (RBD).

(2) As with RBDs, SBU Data Use Requests shall be authorized by the appropriate Authorizing Official (AO). The AO shall not delegate authorizations regarding the acceptability of risk to the agency except where explicitly authorized by another IRM provision or Treasury Directive.

(3) Handling and protection of SBU data must comply with this IRM and PCA's SBU Data Usage and Protection procedures: (internal IRS website) *https://portal.ds.irsnet.gov/sites/vl003/Lists/PrivacyPolicyPrivacyControls/DispItemForm.aspx?ID=16*

(4) Where approval to use SBU data in non-production environments is required, approval will be based on suitable justification and a thorough assessment of the adequacy of mitigation of evident and potential risks.

10.5.8.3
(09-26-2014)
SBU Data Process

(1) Refer to the section Roles and Responsibilities in this IRM for additional guidance on the Authorizing Official and Information Owner.

(2) Ensure the requirements detailed in the Requirements for Using SBU Data section are met.

10.5.8.3.1 (09-26-2014) **Environments**

(1) SBU data might be used in different use case scenarios. The IT security control requirements might differ based on the type of environment. The terms in this section define the environments referred to throughout the IRM. These environments include:

a. **Non-Production IRS environment** – Non-production IRS systems and applications owned or operated by, or on behalf of, the IRS.
b. **Non-IRS environment (planned)** – Non-production vendor (e.g., the non-IRS external entity) environment. This description applies to planned usage of SBU data. These controls apply for the period of time that the SBU data is in the vendor's environment.
c. **Non-IRS environment (unplanned)** – Non-production vendor (e.g., the non-IRS external entity) environment used to respond to unplanned incidents. More than three (3) tickets in six (6) months shall not be treated as unplanned occurrences, but shall use the standard Non-Production IRS environment or Non-IRS environment (planned) process as appropriate.

10.5.8.3.2 (09-28-2015) **Requirements for Using SBU Data**

(1) **Authorization**. The SBU data shall be on an authorized system.
Examples of authorized system include:

a. **ATO or GSS**. Any system with an Authorization to Operate (ATO), such as a General Support System (GSS). If the necessary IT security controls protecting the data are inherited from another application or GSS, then the receiving applications or systems need to be classified at the same FIPS 199 categorization or above unless the IT security controls can be proven to be at the same level as required by the more restrictive classification (e.g., via additional control testing). (See the Equivalency requirement in this section.)
b. **Non-Production IRS Environment**. A test or development environment that meets all requirements in this requirements section.
If the target or receiving environment was not originally authorized with the explicit expectation of processing or storing sensitive information (for example, a test or development system), the appropriate controls for the originating or sending system's FIPS199 classification for the required control families shall be implemented. (See the Equivalency requirement in this section.)

Note: These Non-Production IRS Environment requirements shall apply to planned and unplanned incidents.

c. **Vendor Environment**. Any vendor environment with appropriate agreements and controls in place, outside of IRS physical and/or logical boundaries. Refer to the section IT Security Controls in this IRM. The categories of vendor environments discussed in this IRM are:

-**Planned Vendor Environment**. The vendor shall implement the IT Security Controls listed in this IRM for the protection of SBU data. The vendor should have already implemented most of these controls, as many of the IT Security Controls section of this IRM for SBU data refer to IRS Pub 4812, *Contractor Security Controls* (or IRM 10.8.1, depending on the contractual terms).

-**Unplanned Vendor Environment**. In certain emergency situations (that have an associated Priority One or Two ticket [P1 or P2]), it might be necessary to use SBU data on systems that are not owned or operated on behalf of the federal government (e.g., vendor-owned test systems). Under these circumstances, ensure compliance with the necessary requirements in the IT Security Controls section of this IRM to protect the data, and the AO shall complete the Request in accordance with the procedures detailed in the SBU Data Request Process section of this IRM.

(2) **Approval**. Where SBU data will be transferred from a production environment to a non-production environment, the AO of the receiving (non-production) environment must first obtain approval in accordance with the procedures detailed in the SBU Data Request Process section of this IRM.

(3) **Equivalency**. Security controls must be equivalent or higher than sending environment. The relevant IT Security controls (see IT Security Controls section in this IRM) must be in place.

(4) **Agreements**. When SBU data changes environments, the AO shall ensure these agreements exist:

- If crossing GSSs or environments within the IRS, then a formal shared service arrangement (Memorandum of Understanding (MOU), Memorandum of Agreement (MOA), Data Exchange Agreement, or other vehicle) shall exist, per the requirements of the CA-6 Security Authorization section of IRM 10.8.1.

  Note: In this IRM, a MOU refers to any formal shared service arrangement (Memorandum of Understanding (MOU), Memorandum of Agreement (MOA), Data Exchange Agreement, or other vehicle).

- Any vendor or contractor (hereafter “vendor”) using IRS SBU data must have in place:
  1. A Non-Disclosure Agreement. (NDA)
  2. If IRS SBU data is transferred to a vendor environment, then an Interconnection Security Agreement (ISA) or MOU, as appropriate, shall be implemented to ensure proper protection of the SBU data.
  3. Background investigations on all individuals with access to the SBU data.
  4. An environment with the appropriate IT security controls.

  For additional guidance regarding the NDA and background investigations, refer to:
  - IRM 10.23.2, *Personnel Security, Contractor Investigations*
  - Contractor Security Management: (internal IRS website)*http://awss.web.irs.gov/FMSS/Contractor-Sec-Mgmt/csm-index.html*

  - Background Investigations:*https://nbib.opm.gov/about-us/about-investigations/*

Refer to the section Cybersecurity Architecture & Engineering Advisory A&I Security Engineering Services in IRM 10.8.1 for additional information and support on Interconnection Security Agreements or Memoranda of Agreement.

(5) **Documentation**. Regarding SBU data, the documentation shall exist for:

- A current Privacy and Civil Liberties Impact Assessment (PCLIA; replaced Privacy Impact Assessment (PIA)).
- Need for SBU data (e.g., synthetic/sanitized data not available or sufficient, etc.).
- Information Owner's approval.
- PCA's approval (where required).
- Ongoing maintenance (e.g., recertification requests, additions/removals to access list, changes to environment).
- Final disposition (e.g., removal or destruction) of data.

(6) **Exclusions**. The SBU data shall not be of a type that is not allowed to be sent to a vendor, including:

- Data from classified, investigative, or law enforcement systems.
- Proprietary processes or algorithms used in investigative work.

Refer to these IRMs for details regarding vendor requirements and restrictions regarding where SBU data may be sent:

- IRM 4.60 series, International Procedures.
- IRM 10.2 series, Physical Security.
- IRM 10.23 series, Personnel Security.

(7) **Reintroduction**. SBU data that must be reintroduced shall be prepared for the protection of the data (transit, out-of-network, and return).

a. In the exceptional circumstances when data must be reintroduced to the IRS network, the data integrity shall be verified before being reintroduced to any IRS environments. For example, SBU data replaced with synthetic or sanitized data would need to be converted back to its SBU data form before reintroduction to its original environment.
b. Data from an unsecured environment shall not be returned directly to a production environment.
c. Data shall undergo malware/virus checking and review (such as code, IP, URL).

(8) **Data Security**. The transfer of SBU data shall only be performed through an encryption mechanism such as a virtual private network (VPN) connection that meets FIPS 140-2 validation requirements. (TD P 85-01 S-CT.4)

(9) **Sanctions**. Sanctions shall be included in the contract or an addendum with vendors. Vendors who violate this policy or disclose SBU data shall be subject to sanctions. Sanctions may be as stringent as desired based upon data sensitivity level (i.e., from a warning up to the loss of the contract and/or criminal and/or civil penalties), and might be dictated by the type of SBU data.

Note: Sanctions should be scaled and designed to be meaningful and relevant as to motivate compliance.

10.5.8.3.3 (09-28-2015) Procedure for Requesting Approval to Use SBU Data

(1) The following sections detail the procedures for obtaining approval and documenting the use of SBU data in non-production environments:

- The SBU Data Use Questionnaire, which enables the AO to determine whether completing a SBU Data Use Request is necessary.

- The SBU Data Use Request, which must be completed and signed by the receiving environment AO and approved by both the sending environment IO and PCA.
- The SBU Data Recertification, completed and signed by the receiving environment AO, approved by the sending environment IO, and submitted to PCA.

The forms (SBU Data Use Questionnaire, SBU Data Use Request, and SBU Data Recertification) can be found at: (internal IRS website) *https://portal.ds.irsnet.gov/sites/vl003/Lists/PrivacyPolicyPrivacyControls/DispItemForm.aspx?ID=23*

(2) SBU Data Use Requests may be approved for a period of up to six (6) months unless the project spans at least three (3) years. For projects with a multi-year (three (3) or more years) development plan or ongoing work, renewals may be requested on an annual basis.

10.5.8.3.3.1 (09-26-2014) **SBU Data Use Questionnaire**

(1) The purposes of the SBU Data Use Questionnaire (Form 14664) are:

- To ensure the use of SBU data is necessary.
- To ensure analysis of whether synthetic or sanitized data can replace SBU data.
- To determine whether a SBU Data Use Request is necessary.

(2) Some examples of when the completion of the SBU Data Use Request is not necessary include:

- When the SBU data target environment meets all these requirements:
  - Is within the IRS FISMA inventory.
  - Has an ATO.
  - Meets the requirements in the section of this IRM called Requirements for Using SBU Data.
- When the SBU data target environment is within the FISMA boundary of the sending environment.

Note: Even if the SBU Data Use Request is not necessary, the completed SBU Data Use Questionnaire can supplement security documentation (e.g., SSP) regarding the use (or avoidance) of SBU data.

10.5.8.3.3.2 (09-28-2015) **SBU Data Use Request**

(1) The purposes of the SBU Data Use Request (Form 14665) are:

- To ensure thorough consideration is given to the privacy and security of SBU data prior to use in non-production environments, and that risk is adequately mitigated.
- To document:
  - The use of SBU data (or replacement of SBU data with synthetic and/or sanitized data).
  - The movement or replication of SBU data between environments.
  - The request to use SBU data, giving the IO and PCA the necessary information to allow determination whether to accept the risk of using SBU data.

(2) This documentation provides a detailed description and justification for the use of SBU data, as described in the section Requirement for Using SBU Data in this IRM.

10.5.8.3.3.3
(09-26-2014)
SBU Data Use Recertification

(1) The purpose of SBU Data Use Recertification (Form 14659) is to document the continued use of SBU data (or replacement of SBU data with synthetic and/or sanitized data)

10.5.8.3.4
(09-26-2014)
SBU Data Use Request Process

(1) When requesting SBU data for planned testing, development, or repairs being done in non-production environments (IRS or vendor), the process in the following Planned Uses section must be followed.

(2) Where a mission-critical, unplanned need to use SBU data in a non-production environment (e.g., real-time repairs or analysis of a failure of filing season critical systems) occurs:

a. A P1 or P2 ticket shall be created before any SBU data is transmitted to the non-production environment using the unplanned use policies in this IRM.
b. The process in the following Unplanned Uses section must be followed.

Note: It is understood that it is not always possible to sanitize data, synthesize data, or make a SBU Data Use Request. Under these circumstances, some required sections of the form for the SBU Data Use Request must be completed before the vendor can perform work, while others may be completed later.

(3) If a SBU Data Use Request needs to be reviewed due to changes or renewed, then follow the process in the SBU Data Use Recertification Process section.

10.5.8.3.4.1
(02-20-2018)
Planned Uses

(1) **Questionnaire** (Form 14664) . The receiving environment AO (or delegate, where permitted) shall complete and sign the SBU Data Use Questionnaire prior to completing any first-time SBU Data Use Request. The answers in the Questionnaire document due diligence in trying to avoid the use of SBU data where it is not necessary or alternatives exist. This documentation may be used to supplement the security documentation (e.g., SSP). If the use of SBU data can be avoided, then the AO shall submit the Questionnaire to the IO and PCA through the *Privacy mailbox.

(2) **Request** (Form 14665). The receiving environment AO (or delegate) shall complete and sign the SBU Data Use Request. Refer to the SBU Data Use Request section in this IRM for more information about the form.

(3) **AO Signature**. The receiving environment Authorizing Official (AO) shall sign the completed SBU Data Use Questionnaire and Request: (internal IRS website)
https://portal.ds.irsnet.gov/sites/vl003/Lists/PrivacyPolicyPrivacyControls/DispItemForm.aspx?ID=16
Together, the Questionnaire and Request document the AO's analysis of need for the SBU data, consideration of alternatives (e.g., synthetic or masked data), and justification for the request to use SBU data.

(4) **IO Review**. The AO shall provide the Questionnaire and Request to sending environment's Information Owner (IO).

(5) **IO Determination**. The IO shall make a risk-based determination based on provided information and approve or reject the Request. If approved, IO shall respond to the AO with the signed documents.

(6) **Request Submission**. Once the IO has signed the Request, the AO shall submit the Questionnaire and Request to PCA for review through the *Privacy mailbox.

Note: Completed documents shall be submitted to the *Privacy mailbox **no later than 15 business days before approval to use the SBU data is needed**. Timely approval cannot be guaranteed if this deadline is not met, which might adversely impact scheduling.

(7) **PCA Ruling**. The PCA shall approve or reject the Request. If approved, PCA shall sign the Request and email a signed copy to the requesting AO.

Note: The AO shall be responsible for ensuring that the access roster is kept up-to-date. Removals or additions shall be noted as soon as they are effective, and an updated list shall be sent to the IO and the *Privacy mailbox.

(8) **Recertification** (Form 14659). In planned uses, SBU Data Use Requests shall be approved for a period of up to six (6) months unless the project spans at least three (3) years. For projects with a multi-year (three (3) or more years) development plan or ongoing work, renewals may be done on an annual basis. Where there is an ongoing need for the data beyond the original approval period, the AO must:

a. Complete and sign the form for SBU Data Use Recertification.
b. Obtain the signature of the IO.
c. Submit the completed form to the *Privacy mailbox prior to the original expiration date.

(9) **Disposition**. No later than 15 business days after the expiration date of the approved original or, where applicable, recertification request, the AO shall note on the original signed copy of the request form the manner and date of final disposition (e.g., removal or destruction) of the SBU data and sign the signature box in Section 8.

a. The disposition of data must be made in accordance with IRS standards and practices.
b. Confirmation of final disposition is required for all planned uses.
c. The SBU Data Use Request is not considered closed until the AO confirms final disposition.

(10) **Update**. Send this updated form to both the *Privacy mailbox and the IO.

10.5.8.3.4.2
(09-28-2015)
Unplanned Uses

(1) **AO Signature**. The AO shall sign the completed SBU Data Use Request, completing the sections required for P1 or P2 ticket events, including the associated P1 or P2 ticket number.

Note: Other sections of the form may be completed later, but no later than 10 business days after the closure date of the P1 or P2 ticket.

(2) **Vendor Responsibility**. When the receiving environment is a non-IRS environment, a single person in authority shall be identified at the vendor's receiving environment to take responsibility for the control of the data while being used. This person should have, at a minimum, a Background Investigation and IRS Public trust clearance.

(3) **Scope Definition**. It shall be clearly communicated the scope of the use of the data and the time period that it is approved for use (while the P1 or P2 ticket is open). At no time should this period be granted for more than 15 business days.

Note: This timeframe does not include the disposition or retention time requirements.

(4) **Vendor Personnel**. If vendors will be accessing the SBU data, the following shall be confirmed prior to access:

a. Individuals are covered by an existing Non-Disclosure Agreement (NDA).
b. Background investigations have been done for each individual.
c. Each individual has completed Security Awareness Training (SAT).

(5) **Implement Minimum Controls**. The IT Security Controls in this IRM for unplanned incidents shall be implemented. Any controls pertaining to the system classification listed in the Requirements (see the Equivalency requirement) section of this IRM shall also be implemented.

(6) **Submission to IO**. The signed Request shall be provided to the IO for the IO's signature.

(7) **IO Determination**. IO shall make a risk-based determination based on provided information and approve or reject the Request. If approved, the IO shall sign the Request and return it to the AO.

(8) **Request Documentation**. The AO shall send the Request to the *Privacy mailbox.

(9) **SBU Data Disposal**. All data, metadata, log-files or other derivatives that contain all or part of the SBU data, will be destroyed (in adherence to NIST 800-88) within ten (10) business days after the closure date of the P1 or P2 ticket or any required retention period (as defined by legal or IRS requirements).

(10) **Data Disposal Verification**. The responsible person identified in the Vendor Responsibility step of this section shall document and report back to the AO the manner and date of final disposition (e.g., removal or destruction) of the SBU data.

(11) **Recurrence Likelihood**. The AO shall determine the likelihood of future events requiring the same emergency action. If it is deemed likely, steps should be taken to authorize the remote system to process production data.

(12) **Update**. The AO shall notify PCA and provide all documentation after the P1 or P2 ticket is closed for documentation and justification purposes to ensure proper usage and protection of SBU data no later than 10 business days after the closure date of the P1 or P2 ticket or any required retention period (as defined by legal or IRS requirements) to both the *Privacy mailbox and the IO.

(13) **ISSO Notifications**. The AO shall notify all affected ISSOs of the unplanned transfer of SBU data to or from their respective systems, as well as SBU data removal, reintroduction, and disposition.

10.5.8.3.5 (09-28-2015) SBU Data Use Recertification Process

(1) **AO Approval**. The AO shall sign the completed form for SBU Data Use Recertification (Form 14659)

This form shall include changes from the original SBU Data Use Request.

(2) **Submission to IO**. The signed Recertification shall be provided to the IO for the IO's signature.

(3) **IO Determination**. IO shall make a risk-based determination based on provided information and approve or reject the Recertification. If approved, the IO shall sign the Recertification and return it to the AO.

(4) **Inform PCA**. The AO shall send the Recertification, the updated Questionnaire (if needed), and the original Request to the *Privacy mailbox.

10.5.8.3.6 (09-26-2014) Other Uses of SBU Data

(1) Sensitive data shall be used only as permitted by law and only as necessary.

10.5.8.3.6.1 (02-20-2018) Training

(1) The use of PII, investigative information, or statutorily protected SBU data (e.g., FTI, PHI, Privacy Act) in classroom training is prohibited. The only exceptions are:

- When individuals who have been granted access in accordance with IRS policy perform individual auditable exercises under an instructor's supervision.
- Disclosure approves this usage. Disclosure's page discussing the use of live data during training is: (internal IRS website) *https://portal.ds.irsnet.gov/sites/vl003/Lists/Risksatwork/DispItemForm.aspx?ID=41* (internal IRS website)

(2) Sensitive data may be used by managers during one-on-one on-the-job training of an employee, if the training is in compliance with the statutory requirements or IRS policy (e.g., Unauthorized Access (UNAX) policy and procedures).

10.5.8.3.6.2 (09-26-2014) Research and Statistical Analysis

(1) Research and statistical analysis using SBU data shall be used only as permitted by law and only as necessary in approved production environments.

10.5.8.3.6.3 (09-28-2015) External Organization Investigations or Audits

(1) In authorized investigations or audits, external organizations (e.g., Treasury Inspector General for Tax Administration (TIGTA), General Accounting Office (GAO)) shall be given access to non-production environments containing SBU data to perform their job duties as prescribed where legally permitted.

(2) For additional information, refer to some external entity reference sites:

- Main TIGTA page:
  https://www.treasury.gov/tigta/index.shtml
- If TIGTA calls: (internal IRS website)
  https://portal.ds.irsnet.gov/sites/vl003/lists/uniquesituations/tigta.aspx
- Treasury authorization of TIGTA:
  https://www.treasury.gov/tigta/about_what.shtml
- Main GAO page:
  https://www.gao.gov/

(3) For an investigation, the external organization does not need to request access from PCA.

(4) The external organization shall inform the AO of the receiving environment and provide a list of personnel who require access to the SBU data.

(5) The AO shall add the names of external organization’s personnel who have access to the SBU data to the access list.

(6) The AO shall provide the IO and PCA with the updated access list.

#
#
#
#

#
#
#

#
#
#
#

#
#

#
#

#
#

#
#

#
#

#
#
#
#
#
#
#
#

#
#

#
#

#

#
#
#
#
#

#
#
#

#
#

#
#
#

#
#
#
#

#
#
#

#
#
#
#

#
#
#
#

#
#
#
#
#

#
#
#

#
#
#

#
#
#
#
#

#
#
#

#
#
#
#

#
#
#
#

#
#
#
#
#

#
#
#
#
#
#

#
#
#

#
#
#
#

#
#
#
#

#
#
#
#

#
#
#

#
#
#
#

#
#
#
#

#
#
#

#
#
#
#
#

#
#
#
#

#
#
#
#
#
#

#
#
#
#

#
#
#
#

#
#
#

#
#
#
#
#

#
#
#
#

#
#
#

#
#
#
#

#
#
#
#
#
#

#
#
#

#
#
#
#
#

#
#
#
#
#

#
#
#
#
#
#

#
#
#

#
#
#
#

#
#
#
#

#
#
#

#
#
#
#
#
#

#
#
#

#
#
#
#

#
#
#

#
#

#

#
#
#
#

#
#
#
#

#
#
#
#

#
#
#

#
#
#
#
#
#

#
#
#

#
#
#
#

#
#
#

#
#
#
#

#
#
#
#
#

#
#
#

#
#
#
#

#
#
#

#
#
#
#
#
#

#
#
#

#
#

#
#
#
#
#

#
#
#

#
#
#

#
#
#

#
#
#

#
#
#

#
#
#

#
#
#

#
#
#

#
#
#

#
#
#

#
#
#

#
#
#

#
#
#
#

#

#
#
#
#

#
#
#
#

#
#
#
#

#
#
#
#

#
#
#
#
#
#
#
#
#

#
#
#
#

#
#
#
#

#
#
#

#
#
#

#
#
#
#

#
#
#
#

#
#
#

#
#
#
#
#
#
#
#

#
#
#
#
#
#
#

#
#
#

#
#
#

#
#
#
#
#

#
#
#
#
#

#

#
#
#
#
#
#

#
#
#
#

#
#
#
#

#
#
#

#
#
#
#
#

#
#
#
#
#

#
#
#

#
#
#
#

#
#
#
#

#
#
#
#

#
#
#
#

#
#
#
#
#
#

#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#
#
#

#
#
#
#
#

#
#
#
#

#
#

Exhibit 10.5.8-1 (09-28-2015)
Glossary and Acronyms

Term	Definition or description
AO	Authorizing Official.
ATO	Authorization to Operate.
Authorization To Operate (ATO)	An Authorization to Operate (ATO) is a formal declaration by a Designated Approving Authority (DAA) that authorizes operation of a Business Product and explicitly accepts the risk to agency operations. The ATO is signed after a Certification Agent (CA) certifies that the system has met and passed all requirements to become operational, with a duration of three (3) years.
authorized system	Refer to the Authorization requirement in the Requirements section of this IRM.
Authorizing Official (AO)	The Authorizing Official (AO) or accrediting official, shall be a senior management/ executive official government employee with the authority to formally assume responsibility for operating a system at an acceptable level of risk. (Refer to IRM 10.8.2 for more information.)
CA	Certification Agent.
COTS	Commercial-Off-The-Shelf.
DAA	Designated Approving Authority. For the purposes of this IRM, see Authorizing Official (AO).
Data Owner	See Information Owner.
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. (Title 26—Internal Revenue Code (IRC) § 6103. Confidentiality and disclosure of returns and return information.)
FIPS	Federal Information Processing Standards.
FISMA	Federal Information Security Management Act of 2002.
FTI	Federal Tax Information.
Information Owner (IO)	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
IO	Information Owner.
IRC	Internal Revenue Code.
ISA	Interconnection Security Agreement.
live data	Production data in use.
masked data	See sanitized data.

Exhibit 10.5.8-1 (Cont. 1) (09-28-2015)
Glossary and Acronyms

Term	Definition or description
MOU	Memorandum of Understanding; used in this IRM to refer to any formal shared service arrangement (Memorandum of Understanding (MOU), Memorandum of Agreement (MOA), Data Exchange Agreement, or other vehicle).
NDA	Non-Disclosure Agreement.
NIST	National Institute of Standards & Technology.
non-production	For this IRM, an environment not used as part of a production environment (e.g., testing, development, P1/P2 ticket incidents requiring a vendor's environment for resolution, planned non-production vendor environments) or not having an ATO.
PCA	Privacy Compliance and Assurance.
PCLIA	Privacy and Civil Liberties Impact Assessment.
Personally Identifiable Information (PII)	*Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.* [GAO Report 08-536, Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information, May 2008, *https://www.gao.gov/new.items/d08536.pdf* .] a. To distinguish an individual is to identify an individual, such as with a SSN and Passport Number. However, a list of credit scores without any other information concerning the individual does not distinguish the individual. b. To trace an individual is to process sufficient information to make a determination about a specific aspect of an individual's activities or status, such as with an audit log. c. Linked information is information about or related to an individual that is logically associated with other information about the individual. d. Linkable information is information about or related to an individual for which there is a possibility of logical association with other information about the individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Employees should know that what is non-PII can become PII whenever additional information becomes available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual. [NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII); OMB Memorandum M-10-23] For more information, refer to the PII web page: (internal IRS website) *https://portal.ds.irsnet.gov/sites/vl003/Lists/PII/LandingView.aspx*
PGLD	Privacy, Government Liaison and Disclosure.

Exhibit 10.5.8-1 (Cont. 2) (09-28-2015)
Glossary and Acronyms

Term	Definition or description
PHI	Personal Health Information.
PIA	Privacy Impact Assessment; replaced by Privacy and Civil Liberties Impact Assessment (PCLIA).
PII	Personally Identifiable Information.
Privacy Compliance and Assurance (PCA)	Organization that owns and manages the SBU Data Usage and Protection program for IRS.
production environment	For this IRM, the production environment is the setting where software, data, and other products are actually put into operation for the final intended business function. For example, in a testing environment, a product is still being used theoretically. Users, typically engineers, look for bugs or design flaws. In the production environment, the product has been delivered and needs to work flawlessly. If in doubt, use what the AO determines is the authoritative data set for the functioning of the business environment.
RBD	Risk-Based Decision.
Return	Any tax or information return, estimated tax declaration, or refund claim (including amendments, supplements, supporting schedules, attachments, or lists) required by or permitted under the IRC and filed with the IRS by, on behalf of, or with respect to any person or entity (IRC § 6103(b)(2)(B)).
Return Information	In general, is any information collected or generated by the IRS with regard to any person's liability or possible liability under the IRC. IRC § 6103(b)(2)(A) defines return information as very broad.
sanitized data	Data that has been altered after being extracted from production files to render the data not sensitive.
SBU	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 FOIA (5 U.S.C. 552). SBU data includes but is not necessarily 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, investigation information. • Live data, which is defined as production data in use. Live means that when changing the data, it changes in production. The data may be extracted for testing, development, etc., in which case, it is no longer **live**. Live data often contains SBU. For more information regarding Sensitive But Unclassified (SBU), refer to IRM 10.5.1 and IRM 10.8.1.

Exhibit 10.5.8-1 (Cont. 3) (09-28-2015)
Glossary and Acronyms

Term	**Definition or description**
SP	Special Publication (NIST).
SSP	System Security Plan.
STIG	Security Technical Implementation Guide, from Defense Information Systems Agency (DISA).
synthetic data	Data that does not contain SBU data; however, it imitates data as it appears in an actual taxpayer's file and does not require the submission of a SBU Data Usage and Protection request.
Taxpayer Data	Any information that is obtained or used in the preparation of a tax return (Pub 4557).
TIGTA	Treasury Inspector General for Tax Administration.
UNAX	Unauthorized Access to taxpayer accounts. The Taxpayer Browsing Protection Act (1997) forbids the willful unauthorized access or inspection of taxpayer records. • UNAX: (internal IRS website) *https://portal.ds.irsnet.gov/sites/vl003/Lists/UNAX1/LandingView.aspx* • IRM 10.5.5, *IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance and Requirements*
unsanitized data	Data that has not been altered after being extracted from production files to render the data not sensitive.
vendor	This IRM uses "vendor" to apply to each person or entity contracting with the federal government to provide property, goods, or services. A contract means a mutually binding legal relationship obligating the contractor to furnish the supplies or services (including construction) and the federal executive agency to pay for them.

Exhibit 10.5.8-2 (09-26-2014)
References

Laws, Acts, Mandates, Code, etc.

- Taxpayer Browsing Protection Act (Pub. L. No. 105-35, August 5, 1997; President Clinton).
- USC Title 26, IRC 6103, Confidentiality and Disclosure of Returns and Return Information 6103 of the IRC (26 U.S.C. § 6103).
  Mandates that returns and return information shall remain confidential unless disclosure is authorized by one of the Code's exceptions to confidentiality.
- IRC 7213, IRC 7213A, and IRC 7431:
  - Mandates that returns and return information shall remain confidential unless disclosure is authorized by one of the Code's exceptions to confidentiality.
  - Makes the unauthorized inspection of Federal Tax Information (FTI) to be a misdemeanor, punishable by fines, imprisonment, or both.
  - Prescribes civil damages for unauthorized inspection or disclosure, and upon criminal indictment or information under IRC 7213 or IRC 7213A, notification to the taxpayer that an unauthorized inspection or disclosure has occurred.

- OMB Memo M-04-04.
- OMB Memo M-06-16.
- E-Authentication Guidance for Federal Agencies.
- E-Government Act of 2002, Section 208 (Public Law 107-347, 44 U.S.C. Ch 36).
- Freedom of Information Act (FOIA).
- NARA General Records Schedules (GRS) provide federal policy on record retention.
- National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 1000, National Information Assurance Certification and Accreditation (C&A) Process (NIACAP) for IRS information systems handling national-security information.

IRS

- **Cybersecurity**: (internal IRS website)
  https://portal.ds.irsnet.gov/sites/CyberSRM/SitePages/Home.aspx
- **Authorized software**: (internal IRS website)
  http://ea.web.irs.gov/esp/default.aspx
- **Office of Disclosure**:
  https://portal.ds.irsnet.gov/sites/vl003/pages/home.aspx?bookshelf=disclosure
- **Office of Safeguards**:
  SafeguardReports@irs.gov
  https://portal.ds.irsnet.gov/sites/vl003/Lists/Safeguards/LandingView.aspx
- **Privacy, Governmental Liaison and Disclosure**: (internal IRS website)
  https://portal.ds.irsnet.gov/sites/vl003/
- **SA&A**: (internal IRS website)
  https://portal.ds.irsnet.gov/sites/CyberSRM/Public/SitePages/SAA.aspx

Related IRMs:

- IRM 1.15 series, *Records and Management*.
- IRM 2.7.4 – *Modernization and Information Technology Services (MITS) Operations, Magnetic Media Management*.
- IRM 2.14 series, *Asset Management*
- IRM 2.27.1, *Configuration Management*, *Configuration Management*.
- IRM 10.2 series, *Physical Security Program*

Exhibit 10.5.8-2 (Cont. 1) (09-26-2014)
References

- IRM 10.5.5, *IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance and Requirements*.
- IRM 10.6 series, *Continuity Operations*.
- IRM 10.8.1 – *Information Technology (IT) Security, Policy and Guidance*.
- IRM 10.8.2 – *Information Technology (IT) Security, Roles and Responsibilities*.
- IRM 10.8.3 – *Information Technology (IT) Security, Audit Logging Security Standards*.
- IRM 10.8.26 – *Information Technology (IT) Security, Mobile Computing Device Security Policy*.
- IRM 10.8.40 – *Information Technology (IT) Security, Wireless Security Policy*.
- IRM 10.8.52 – *Information Technology (IT) Security, PKI Security Policy*.
- IRM 10.8.60 – *Information Technology (IT) Security, IT Service Continuity Management (ITSCM) Policy and Guidance*.
- IRM 10.8.62 – *Information Technology (IT) Security, Information Systems Contingency Plan (ISCP) and Disaster Recovery (DR) Testing, Training, and Exercise (TT&E) Program.*
- IRM 11.3 series, *Disclosure of Official Information*.
- Publication 4812, *Contractor Security Controls: Handling and Protecting Information or Information Systems*

NIST

- NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
- NIST SP 800-30 Rev 1, *Guide for Conducting Risk Assessments*, September 2012.
- NIST SP 800-37 Rev 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, February 2010.
- NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002.
- NIST SP 800-53 Rev 4, *Recommended Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013.
- NIST SP 800-53A Rev 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, June 2010.
- NIST SP 800-88, *Guidelines for Media Sanitization*, September 2006.
- NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010.

Treasury

- TD P 80-05, *Records and Information Management Program*, June 2002.
- TD P 85–01, *Treasury Information Technology (IT) Security Program*, April 4, 2014.