



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

4.33.1

SEPTEMBER 1, 2020

EFFECTIVE DATE

(09-01-2020)

PURPOSE

- (1) This transmits new IRM 4.33.1, Electronic Business, Managing Electronic Records from Taxpayers and Third Parties.

MATERIAL CHANGES

- (1) This new IRM section provides guidance with respect to the handling of electronic records for Small Business and Self-Employed (SB/SE) Field Examination and Specialty Examination employees.

EFFECT ON OTHER DOCUMENTS

None.

AUDIENCE

Small Business/Self-Employed (SB/SE) Field Examination and Specialty Examination employees

Maha H. Williams
Director, Examination - Field and Campus Policy
Small Business/Self-Employed

4.33.1

Managing Electronic Records from Taxpayers and Third Parties

Table of Contents

4.33.1.1 Program Scope and Objectives

4.33.1.1.1 Background

4.33.1.1.2 Authority

4.33.1.1.3 Roles and Responsibilities

4.33.1.1.4 Terms and Acronyms

4.33.1.1.5 Related Resources

4.33.1.2 Requesting Electronic Records - IDR and Summons

4.33.1.3 Receiving Electronic Records

4.33.1.4 Accessing Electronic Records

4.33.1.4.1 Encrypted Electronic Records

4.33.1.5 Preserving Original Records and Creating Working Copies

4.33.1.6 Maintaining and Storing Electronic Records Containing SBU Information

4.33.1.6.1 Storing Portable Storage Devices (PSDs)

4.33.1.7 Transmitting Electronic Records

4.33.1.7.1 Shipping Portable Storage Devices (PSDs)

4.33.1.8 Closing Cases with Electronic Records

4.33.1.8.1 Labeling and Location of Portable Storage Devices (PSDs)

4.33.1.8.2 Referencing Electronic Files Stored on Portable Storage Devices (PSDs)

4.33.1.8.3 Documenting Contents of Portable Storage Devices (PSDs)

4.33.1.9 Disposing of Electronic Records

4.33.1.9.1 Disposing of Portable Storage Devices (PSDs)

4.33.1.1 (09-01-2020) Program Scope and Objectives

- (1) **Purpose.** This IRM provides procedures for requesting, receiving, preserving, maintaining, storing, controlling, transmitting, and disposing of electronic records received during an examination in accordance with IRM 10.8.1, Policy and Guidance; the IRM 1.15, Records and Information Management, series; and the IRM 10.2. Physical Security Program, series.
- (2) **Audience.** These procedures apply to employees in SB/SE Field Examination and SB/SE Specialty Examination.
- (3) **Policy Owner.** The Director, Examination - Field and Campus Policy, who is under the Director, Headquarters Examination.
- (4) **Program Owners.**
 - The Director, Examination - Field and Campus Policy, is responsible for guidance and procedures related to the SB/SE examination process.
 - The Records and Information Management (RIM) office, under Privacy, Governmental Liaison and Disclosure (PGLD) is the program office responsible for oversight of the Servicewide records management policy.
 - Collection Policy Headquarters, an organization within the Small Business/Self-Employed (SB/SE) division, is the program office responsible for guidance and procedures related to summonses.
 - Information Technology (IT) is responsible for delivering IT services and solutions and establishing the security program and the policy framework for the IRS.
- (5) **Contact Information.** To recommend changes or make any other suggestions related to this IRM, see IRM 1.11.6.6, Providing Feedback About an IRM Section - Outside of Clearance.

4.33.1.1.1 (09-01-2020) Background

- (1) Various types of electronic records are defined in IRM 1.15.6.2, Basic Electronic Records Management Definitions. An electronic record contains information recorded in a form that is machine-readable (e.g., information that only a computer can process, and which, without a computer, would not be understandable to people). During an examination, examiners receive various types of electronic records, including accounting software data, bank account information, workpapers, invoices, e-payment provider records, logs, etc. This IRM provides guidance for the handling of electronic records.

4.33.1.1.2 (09-01-2020) Authority

- (1) By law, the Service has the authority to conduct examinations under Title 26, Internal Revenue Code, Subtitle F – Procedure and Administration, Chapter 78, Discovery of Liability and Enforcement of Title, Subchapter A, Examination and Inspection, which includes, but is not limited to, IRC 7602, Examination of Books and Witnesses.

Note: Additional authority for conducting examinations is contained in the 26 CFR 601.105, Statement of Procedural Regulations, and 26 CFR 301.7602-1, Examination of Books and Witnesses.
- (2) Rev. Rul. 71-20, Notice or Regulations Requiring Records, Statements, and Special Returns, 26 CFR 1.6001-1, provides guidance that punched cards, magnetic tapes, disks, and other machine-sensible data media used in the

automatic data processing of accounting transactions constitute records within the meaning of 26 CFR 1.6001-1 of the regulations.

- (3) Rev. Proc. 98-25, Examination of returns and claims for refund, credits or abatement; determination of correct tax liability, provides the basic requirements that the Internal Revenue Code considers to be essential in cases where a taxpayer's records are maintained within an Automatic Data Processing system (ADP).
- (4) Rev. Proc. 97-22, Examination of returns and claims for refund, credits or abatement; determination of correct tax liability, provides guidance to taxpayers who maintain books and records using an electronic storage system.

4.33.1.1.3 (09-01-2020) **Roles and Responsibilities**

- (1) The Director, Headquarters Examination, is the executive responsible for providing policy and guidance for SB/SE Examination employees and ensuring consistent application of policy, procedures, and tax law to effect tax administration while protecting taxpayers' rights. See IRM 1.1.16.3.5, Headquarters Examination, for additional information.
- (2) The Director, Examination - Field and Campus Policy, reports to the Director, Headquarters Examination, and is responsible for the delivery of policy and guidance that impacts the examination process. See IRM 1.1.16.3.5.1, Field and Campus Policy, for additional information.
- (3) Field Exam General Processes (FEGP), which is under the Director, Examination - Field and Campus Policy, is the group responsible for providing policy and procedural guidance on standard examination processes to field employees. See IRM 1.1.16.3.5.1.1, Field Exam General Processes, for additional information.
- (4) All examiners must perform their professional responsibilities in a way that supports the IRS Mission. This requires examiners to provide top quality service and to apply the law with integrity and fairness to all.
- (5) Examiners and their managers should thoroughly acquaint themselves with the examination procedures and information contained in this IRM, as well as other resources, such as those listed in IRM 4.33.1.1.5.

4.33.1.1.4 (09-01-2020) **Terms and Acronyms**

- (1) The following table contains a list of terms used throughout this IRM.

Term and Acronym	Definition
Accounting Software	A type of application software that records and processes accounting transactions with functional modules (e.g., accounts payable, accounts receivable, general journals and other ledgers).
Accounting Software Data File	A file from an accounting software program that contains numeric, textual, or graphic information, but not code, that is organized in a strictly-prescribed file and format. These files are meant to be read or viewed, but not executed. Accounting Software Backup Files are one type of Accounting Software Data File.

Term and Acronym	Definition
Compact Disk (CD)	A circular optical disk that is approximately 4.75 in (12 cm) in diameter capable of storing digital data. A CD is a type of Portable Storage Device (PSD).
Computer Security Incident Response Center (CSIRC)	Responsible for monitoring the IRS network 24 hours a day year-round for cyber attacks and computer vulnerabilities and for responding to various security incidents such as the theft of a laptop computer.
Digital Versatile Disk (DVD)	A type of optical disk used for storing digital data. It is the same size as a CD but has a larger storage capacity. A DVD is a type of Portable Storage Device (PSD).
Download	The act of transmitting information (software, data, etc.) from one device to another.
Email (Electronic Mail)	A record created or received on an email system, including any attachments which may be transmitted with the message.
Encryption	Any procedure used to convert plaintext into ciphertext to prevent anyone but the intended recipient from reading that data. The Service currently uses several methods of encryption based on the task at hand.
Executable File	A type of file that, when opened, is used to perform various functions or operations on a computer. Common executable file extensions include, but are not limited to, .bat, .com, .dmg, .exe, .msi, .vb.
External Hard Drive	A portable storage device that can be attached to a computer through a universal serial bus (USB) cable or wireless connection. An external hard drive is usually used to store media that a user needs to be portable, for backups, or when the internal drive of the computer is already at its full storage capacity.
Financial Software	A type of software designed to automate, assist and store financial information of a personal or business nature. The software handles the analysis, management, processing, and storage of a set of financial processes, records and transactions.
Information Technology (IT)	The application of computers and telecommunications equipment to store, retrieve, transmit, and manipulate data, often in the context of a business or other enterprise.
Instant Message (IM)	Electronic message with a short-term business need (transitory). Examples of instant messaging systems include Microsoft Office Skype for Business®, Office Communications Server® (OCS), and Lync®.
Issue Management System (IMS)	The system/application used by Specialty Tax for case management.
Memory Card, Flash Card, or Memory Cartridge	A portable storage device used for storing digital information. They are typically small in size and are commonly used in small portable devices such as cameras and phones.
Metadata	Detail embedded in electronic data that describes how, when, and by whom a the data was collected, created, accessed, modified, and formatted.

Term and Acronym	Definition
Optical Disk	A portable storage device that can be inserted into an optical disk reader. The most common types of optical disk are the compact disk (CD) and digital versatile disk (DVD).
Portable Electronic Device (PED)	Any non-stationary electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images. This includes, but is not limited to: laptops, cellular telephones, thumb drives, video cameras, and pagers.
Portable Storage Device (PSD)	<p>A device that stores electronic information and can be connected to a computer to download or upload information. Portable Storage Devices (PSDs) are a subset of Portable Electronic Devices (PEDs), hence all PED security controls also apply to PSDs. The four basic types of PSDs are the optical disk, universal serial bus (USB) flash drive, flash memory card, and external hard drive. PSDs are sometimes referred to as "storage media."</p> <p>Note: The most common PSDs are CDs, DVDs, and thumb drives.</p>
Report Generation Software (RGS)	The software program used in the income tax examination process to compute corrected tax, penalties, interest; generate examination reports, supporting schedules, and various published forms and letters; store case documents, including reports, lead sheets, workpapers, letters and other electronic documents critical to the case; and post examination results and archive cases.
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. See IRM 10.5.1.2.2, Sensitive But Unclassified (SBU) Data.
Standalone	A desktop or laptop computer that is used on its own without requiring a connection to a network. A system that does not require a connection to any other computer for it to use an application (e.g., word processor or spreadsheet program); instead, the application programs stored on its hard drive are used. A standalone computer may be equipped with a printer, scanner, or external zip or hard drive.
Symantec Endpoint Encryption (SEE)	<p>Software tool that encrypts all IRS laptops' hard drives to prevent unauthorized access and ensures the security of IRS personal computers and data. The SEE password screen is the first screen you see when you start or reboot your laptop. The SEE software also includes the following applications:</p> <ul style="list-style-type: none"> • SEE Access Utility - An application that allows a taxpayer or other third party to access password-encrypted files on a PSD. The access utility application is automatically copied to all removable storage devices when attached to an IRS computer. • SEE Removable Storage (SEERS) - IRS IT-approved encryption tool used to encrypt files copied or moved to PSDs. SEERS is the replacement for Guardian Edge Removable Storage (GERS). For additional information, see IRM 10.5.1.6.2.1, External.

Term and Acronym	Definition
Uniform Resource Locator (URL)	A reference (web address) to a resource (such as a document or website) on the internet.
Universal Serial Bus (USB)	An industry standard developed in the mid-1990s that defines the cables, connectors, and communication protocols used in a bus for connection, communication, and power supply between computers and electronic devices.
Universal Serial Bus (USB) Storage Device	A portable storage device that includes flash memory with an integrated USB interface. USB storage devices are typically 1-2 inches long, weigh less than 3 ounces, and are connected to the computer through a USB port. Other names for a USB storage device are thumb drive, pen drive, jump drive, key chain drive, flash drive, and memory stick.
Wireless	A technology that enables devices to communicate without physical connections (without requiring network or peripheral cabling).

4.33.1.1.5
(09-01-2020)

(1) The table provides additional IRM resources related to electronic records.

Related Resources

IRM	Title	Guidance for
IRM 1.15.2.2	Definition of Records	Statutory definition of the term "record."
IRM 1.15.6	Managing Electronic Records	The creation, maintenance, use, and disposition of federal records created using IRS electronic information systems and personal computers, including email and other electronic applications.
IRM 4.10.4.3.7.5	Evaluating Electronic Books and Records	Basic requirements examiners should consider when reviewing and evaluating taxpayer's electronic records.
IRM 4.10.9	Workpaper System and Case File Assembly	Developing lead sheet and workpaper content, and case file organization. These guidelines are provided to promote quality and consistency in the preparation and completion of lead sheets, workpapers, and case.
IRM 4.10.15	Report Generation Software (RGS)	Using RGS to compute corrected tax, interest, penalties and generate audit reports, create various forms and letters, allow examiners to document actions and findings, and process and archive examination results.
IRM 4.23.4.4	Guide for Examiners Using Issue Management System (IMS)	Guidance for employment tax examiners on the use of the Issue Management System (IMS). Use of IMS is required for all employment tax audits by employment tax examiners.
IRM 4.24.6.2	Excise Issue Management System (IMS)	Case management tool required for all excise examinations.

IRM	Title	Guidance for
IRM 4.25.1.8	Issue Management System (IMS)	Case management tool required for all Estate & Gift examinations.
IRM 10.2.14	Methods of Providing Protection	Methods of protection to IRS controlled space and information.
IRM 10.2.15	Minimum Protection Standards (MPS)	Minimum standards for protecting data and items requiring safeguarding.
IRM 10.5.1	Privacy Policy	Protecting the privacy of Sensitive But Unclassified (SBU) data for taxpayers and employees, including personally identifiable information (PII) and tax information.
IRM 10.8.1	Policy and Guidance	All aspects of security for the protection of IT resources to be followed by all IRS organizations.
IRM 10.8.1.4.10.3	MP-4 Media Storage	Requires all information system media be protected until media is destroyed or sanitized. IRM 10.8.1.4.10.3.1, Portable Electronic Devices (PEDs) as Storage Media, provides these controls apply to any device having internal storage that can be connected to a computer and used to download or upload information.
IRM 10.8.1.4.10.6	MP-7 Media Use (InTC)	Media provided by taxpayers and other IRS business partners shall be handled with minimum security controls, including running virus scan of the media.
IRM 10.8.27	Personal Use of Government Furnished Information Technology Equipment and Resources	Allowable minimum standard regarding the acceptable personal use of government furnished IT equipment and resources by IRS employees, contractors, vendors, and outsourcing providers.
IRM Exhibit 10.8.27-1	Prohibited Uses of Government Furnished IT Equipment and Resources	Provides examples of some prohibited uses of government furnished IT equipment and resources. IRM Exhibit 10.8.27-1(9), Prohibited Uses of Government Furnished IT Equipment and Resources, provides restrictions related to unauthorized applications or data programs (e.g., executable code).
IRM 11.3.1.17.2	Electronic Mail and Secure Messaging	Provides rules for email and secure messaging.
IRM 11.3.13	Freedom of Information Act (FOIA)	Processing requests for records maintained by IRS.
IRM 25.3.1.7	Preserving Electronically Stored Information In Litigation Cases	Background and instructions on electronically stored information and its use in litigation cases.
IRM 25.5.2	Preparation	Preparation of summonses.
IRM 25.5.3.5	Records on Encrypted Storage Media	Retrieving, handling, and destroying electronic records received on encrypted storage media in response to summons.

IRM	Title	Guidance for
IRM 25.5.3.6	Electronic Summons Processes	Electronic service of summons, electronic retrieval of records, accessing records through a URL, and saving records for the administrative case file.
IRM 25.5.9.6	Information Received by Electronic Storage Media	Payment of summons received via electronic storage media; procedures when payment is requested for both electronic and paper documents.
IRM 25.5.9.7	Information Received by Electronic Transmission	Payment of summons when received via electronic transmission; procedures when payment is requested for paper documents when summoned information is provided via electronic transmission.

(2) Helpful resources are as follows:

- *IRS Computer Incident Response Center (CSIRC)* (<https://www.csirc.web.irs.gov>)
- *IRS CSIRC Contact Information* (<https://www.csirc.web.irs.gov/about/contact.html>)
- *Computer Security Incident Reporting Procedures* (https://www.csirc.web.irs.gov/reporting/Incident_Reporting_Procedures.pdf)
- *Computer Security Incident Reporting Form* (<https://www.csirc.web.irs.gov/incident/>)
- *Internet Proxy Exception Request Form* (<https://www.csirc.web.irs.gov/block/>) - Form used to request exception to a blocked site.
- *Disclosure and Privacy Knowledge Base* (<https://portal.ds.irsnet.gov/sites/vl003/pages/default.aspx>)
- *Electronic Records Document Requests* (<http://mysbse.web.irs.gov/examination/tip/elrcgninfo/docrequests/default.aspx>)
- *Summons Attachments* (<https://portal.ds.irsnet.gov/sites/vl019/lists/summonsattachments/landingview.aspx>)
- *Encryption* (<https://portal.ds.irsnet.gov/sites/vl003/Lists/PrivacyPolicyPrivacyControls/DispItemForm.aspx?ID=18&Source=https%3A%2F%2Fportal%2Eds%2Eirsnet%2Egov%2Fsites%2Fvl003%2Flists%2Fprivacypolicyprivacycontrols%2Fencryption%2Easpx&ContentTypeId=0x010041B8C41117689442BE9634D5192DA713>)
- *Electronic Records - General Information* (<http://mysbse.web.irs.gov/examination/tip/elrcgninfo/default.aspx>)
- *Symantec Endpoint Encryption* (<https://irssource.web.irs.gov/Lists/IT4U/DispItemForm.aspx?ID=92&Source=https%3A%2F%2Firssource%2Eweb%2Eirs%2Egov%2Flists%2FIT4U%2FAllItems%2Easpx&ContentTypeId=0x0100659B9D86D45FF840849295799B403683>)
- *How to Run a Virus Scan* (<http://mysbse.web.irs.gov/examination/tip/elrcgninfo/jobaids/22010.aspx>)
- *QuickBooks* (<http://mysbse.web.irs.gov/examination/tip/quickbooks/default.aspx>)
- *Sage Software* (<http://mysbse.web.irs.gov/examination/tip/peachtree/default.aspx>)
- *QuickBooks/Sage Software-For All Examiners* (<https://organization.ds.irsnet.gov/sites/SBSEfeER/HQ/Software/SitePages/Home.aspx>)

- *RGS - Report Generation Software* (<http://mysbse.web.irs.gov/examination/rgs/default.aspx>)
- *Issue Management System (IMS) Server Status* (<https://irssource.web.irs.gov/LBI/SitePages/IMS.aspx>)
- *Summons Knowledge Base* (<https://portal.ds.irsnet.gov/sites/vl053/pages/default.aspx>) - Collection page
- *eSummons* (<https://portal.ds.irsnet.gov/sites/vl053/pages/home.aspx?bookshelf=esummons>)
- *Electronic Retrieval of Summoned Records Using a URL* (<https://portal.ds.irsnet.gov/sites/vl053/Lists/Portals/DispItemForm.aspx?ID=6&Source=https%3A%2F%2Fportal%2Eds%2Eirsnet%2Egov%2Fsites%2Fvl053%2Flists%2Fportals%2Flandingview%2Easpx&ContentTypeId=0x01005AA9FB0D41E54642B37275BFCB2AF84A>)
- *Summoning* (<https://portal.ds.irsnet.gov/sites/vl019/pages/home.aspx?bookshelf=summonsing>) - (Fraud Development Knowledge Base Site)
- *Third-Party Contacts* (<https://portal.ds.irsnet.gov/sites/vl051/lists/thirdpartycontacts1/landingview.aspx>)
- **SBSE E-Summons Decryption Team* (sbse.e.summons.decry@irs.gov) - Mailbox used to request assistance with encrypted electronic records, questions on electronic summons processes, or if you are unsure if a website is secure to download records provided as a result of a summons.

4.33.1.2 (09-01-2020)

Requesting Electronic Records - IDR and Summons

- (1) During the initial conversation, examiners should ask the taxpayer about their use of electronic records, including accounting software. If the taxpayer uses electronic records the examiner should request them early in the examination, as well as user names and passwords necessary to read the electronic files, using Form 4564, Information Document Request (IDR).

Note: See *Electronic Records Document Requests* for Counsel approved language to request certain accounting software data files on an IDR or summons.

- (2) If a taxpayer does not voluntarily provide requested electronic records, the examiner should consider issuing a summons to the taxpayer or a third party (e.g., preparer, financial institution) that may have access to the electronic records. To prevent potential defenses the taxpayer may raise if they petition to quash the summons, the language included in the summons should closely resemble the language that was included in the IDR issued to the taxpayer. IRM 25.5, Summons, provides Servicewide summons guidance. See IRM 25.5.2, Preparation, for information related to preparation of summonses and IRM 25.5.3.6, Electronic Summons Process, for more information on the electronic summons process.

Caution: Third-party contact notification procedures must be followed before issuing a third party summons. See *Third Party Contacts* for current guidance.

4.33.1.3 (09-01-2020)

Receiving Electronic Records

- (1) Electronic records are received in several ways. Employees should not refuse to accept electronic records, whether they are encrypted or not; however, necessary precautions must be taken to safeguard the data, IRS computers, and the IRS network.
- (2) Taxpayers and their representatives provide electronic records by:

- a. **Email** - Employees must advise taxpayers and their representatives that the Service cannot guarantee the security of their information if they choose to send it by email. For guidance regarding transmitting emails with SBU content, see IRM 4.33.1.7.

Caution: If examiners receive unsolicited emails from taxpayers or their representatives, respond by letter or phone if an address or phone number is available. Examiners should discourage the taxpayer or their representatives from continuing the discussion by email. See IRM 10.5.1.6.8.1(3), *Emails to Taxpayers and Representatives*.

- b. **Portable Storage Devices** - When electronic records are received on PSDs, employees must follow procedures to protect IRS computers and the IRS network before accessing the records. See IRM 4.33.1.4 for guidance on accessing records stored on PSDs.

- (3) Summoned third parties may ask examiners to retrieve records through an electronic summons website. See IRM 25.5.3.6.2, *Electronic Retrieval of Records*. For additional information, refer to *eSummons* and *Sources that Respond Electronically* for approved electronic summons processes.

4.33.1.4 (09-01-2020) Accessing Electronic Records

- (1) Examiners must complete the following actions when electronic records are **received on a PSD**:

- a. Follow procedures in IRM 10.8.1.4.10.6(4)(a) through (d), MP-7 Media Use (InTC), regarding virus scans. Document virus scan actions on the Form 9984, Examining Officer's Activity Record, or RGS/IMS Case History.

Note: See job aid, *How to Run a Virus Scan*, for additional guidance on scanning PSDs for viruses.

Caution: If a virus is detected, do **not** reconnect the computer to the IRS network and do **not** power-down or reboot the computer. Within one (1) hour of detection, the examiner must contact their manager and CSIRC. See IRM 10.8.1.4.10.6(4)(d), MP-7 Media Use (InTC), and *IRS Computer Security Incident Reporting Procedures*.

- b. Save the files to an encrypted folder on the examiner's computer. If it is not possible to immediately save the information to the computer, it must be done at the earliest opportunity.
- c. Document all actions taken with electronic records as described in IRM 4.33.1.5.

- (2) Examiners must complete the following actions when electronic records are **received via email**:

- a. Save the files to an encrypted folder on the examiner's computer. If it is not possible to immediately save the information to the computer, it must be done at the earliest opportunity.
- b. Document all actions taken with electronic records as described in IRM 4.33.1.5.

- (3) Electronic records are generally readable if they are in a format that uses a standard software program (e.g., Word, Excel, Access, Adobe). If the electronic records are not readable, specialists are available to assist with accessing records. For a description of the specialists and how to locate each type of specialist, see the article *Who do I contact for assistance?*.
- (4) Do not open executable files or software applications provided by external parties, including decrypting applications and proprietary applications needed to read data files, as the file may contain a virus that could infect the computer and IRS network. If a file requires the running of an executable file or software in order to access it, see IRM 4.33.1.4.1 (2)(b) and (c) and IRM 25.5.3.5(4), Records on Encrypted Storage Media, for guidance on who to contact for assistance. See also IRM Exhibit 10.8.27-1(9), Prohibited Uses of Government Furnished IT Equipment and Resources, for restrictions related to unauthorized applications or data programs (e.g., executable code).

4.33.1.4.1
(09-01-2020)
**Encrypted Electronic
Records**

- (1) If encrypted electronic records are received, examiners must store the password which decrypts the data file separately from the electronic records. See IRM 4.33.1.5 (7) for information related to documenting user names and passwords.
- (2) Some third parties (such as banks) provide data on an encrypted PSD (e.g., CD, DVD, USB storage device). There are three main categories of encrypted electronic records (i.e., data files) that may be provided:
 - a. **Records Not Requiring Software Installation or Running Self-Decrypting Executable Files** - Some data files do not require installation of encryption or viewer software programs or the running of self-executable files. When these files are encrypted, they usually require a password without double-clicking on an executable file and are generally safe to access. Examples include password protected Adobe (.pdf) and SecureZIP (.zip) files.
 - b. **Records Requiring Installation of Software Programs** - These data files require the installation of an encryption or viewer software program created or purchased by the provider. Do **not** install software on IRS computers that has not been properly tested by IT, as the file may contain a virus that could infect the computer and IRS network. See IRM 10.8.1, Policy and Guidance, and IRM 10.8.27, Personal Use of Government Furnished Information Technology Equipment and Resources, which provides the restriction on downloading and installing unauthorized programs or software from the internet. Executable downloads occur when executable files are run and code is automatically executed that often installs and runs programs. Common executable file extensions include .bat, .com, .dmg, .exe, .msi, .vb, however there are many others. For assistance with decrypting these types of data files or questions as to whether or not a data file can be opened, send an email to **SBSE E-Summons Decryption Team* with the required information described in IRM 25.5.3.5(4), Records on Encrypted Storage Media.
 - c. **Records Running Self-Decrypting Executable Files** - Some data files require self-decrypting files be run by double-clicking on an executable file which prompts the user to enter a password. These files may not always appear to be executable files since the software needed to read the file does not need to be installed, therefore examiners must view the file extension to determine if it is a common executable file (e.g., .bat, .com, .dmg, .exe, .msi, .vb). Do **not** run or execute these types of files, as the

files may contain viruses that could infect the computer and IRS network. For assistance with decrypting these types of data files or questions as to whether or not a data file can be opened, send an email to **SBSE E-Summons Decryption Team* with the required information described in IRM 25.5.3.5(4), Records on Encrypted Storage Media.

4.33.1.5
(09-01-2020)
**Preserving Original
Records and Creating
Working Copies**

- (1) Examiners must document all actions regarding electronic records on Form 9984, Examining Officer's Activity Record, or RGS/IMS Case History to document the chain of custody. Documentation must include:
 - Date of receipt.
 - Name of person who provided the records.
 - How the records were obtained (e.g., received on PSD).
 - Format of data received (e.g., .docx, .xlsx, .pdf, etc).
 - A statement that the original records have not been altered by the examiner.
- (2) IRM 1.15.2.2, Definition of Records, describes the statutory definition of a federal **record** pursuant to 44 U.S.C. § 3301. This definition includes most electronic records received from taxpayers. Federal records, whether electronic or paper, must be retained according to the National Archives and Records Administration (NARA) approved disposition authority or printed and associated with the appropriate recordkeeping system (e.g., case file, RGS, IMS). Unlawfully destroying federal records is a violation of the Federal Records Act and carries stiff penalties. See IRM 1.15.6.9, Retention and Disposition of Electronic Records.
- (3) Email messages determined to be federal records are subject to retention policies and can be deleted only when they are eligible for destruction or when they have been printed to paper or PDF and associated with the appropriate recordkeeping system. IRM 1.15.6, Managing Electronic Records, provides guidance regarding the creation, maintenance, use, and disposition of federal records created using IRS electronic information systems and personal computers, including email and other electronic applications. See IRM Exhibit 1.15.6-1, Common Questions about Email, for information on when an email message is considered a federal record.

Caution: See IRM 4.33.1.9 for guidance on disposing electronic records.

- (4) Instant messaging should not be used to engage in discussions regarding business decisions related to examinations. If instant messaging is used in these situations, the result is a federal record and the message must be saved, printed to paper or PDF, and associated with the appropriate recordkeeping system. See IRM 1.15.6.14.1(3), Use of Agency-approved Electronic Messaging Systems, and IRM 1.15.6.14.2(2)(b) and (c), Preserving Electronic Messages. Also see IRM Exhibit 1.15.6-2, Common Questions about Electronic Messaging, for information on when an instant message is considered a federal record and how to save instant messages.
- (5) Electronic records received from a taxpayer, third party, or other stakeholder and copied to an examiner's computer are considered "original" files. Do not edit the original files. The original files must be maintained in accordance with IRM 4.33.1.6.

- (6) Examiners should use original records only to create “working” copies. Once working copies are created, avoid using the original records except to make additional working copies if necessary. The working copies should be used for analysis, documentation, etc. The working copies must be maintained in accordance with IRM 4.33.1.6. Use of a working copy may include, but is not limited to:
 - a. Sorting and analyzing records using Microsoft Word, Excel, or Access.
 - b. Opening and reading data files using the related accounting or financial software.
- (7) Examiners should record user names and passwords for all PSDs on Lead Sheet 100-1A, External Records Password. The lead sheet must also include a description of the type of data (e.g., summoned records, accounting software files) and the encryption method used (e.g., SecureZip, Symantec Endpoint Encryption Removable Storage [SEERS]). For guidance on creating passwords, see IRM 10.8.1.4.7.4.1, IA-5 Authenticator Management - Control Enhancements.
- (8) See IRM 4.33.1.6 for additional information on maintenance and storage of electronic records.

4.33.1.6
(09-01-2020)
**Maintaining and Storing
Electronic Records
Containing SBU
Information**

- (1) As noted in IRM 4.33.1.5 (5) and (6), the examiner conducting the examination is responsible for maintaining “original” and working copies of electronic records received from taxpayers, representatives, or other parties. Original and working copies can be maintained on the examiner’s hard drive or on an encrypted PSD until they are no longer needed. See IRM 4.33.1.8 for information on when to include electronic files with the closed case file.

Note: All PSDs must be physically controlled and secured at all times. See IRM 4.33.1.6.1.

- (2) Taxpayer data copied and maintained on PSDs must be encrypted using the current IRS IT-approved encryption program (i.e., SecureZip, SEERS) and must be password protected per IRM 10.5.1.6.2.1, External. See IRM 4.33.1.5 (7) for guidance on recording and storing passwords for cases worked in RGS.

Caution: See IRM 4.10.15.7.19(6)(c), Office Documents and Case File Documents, for guidance on storing files over 5 MB in RGS.

- (3) Employees must always save Sensitive But Unclassified (SBU) data in the designated encrypted SBU folder of their computer.

Note: Per IRM 4.10.9.7.11.1(3), Electronic Accounting Software Backup Data Files and Spreadsheets, accounting software data files are not compatible with RGS. As such, examiners must store such files in the encrypted SBU folder on the their computer or on an encrypted PSD.

- (4) To prevent data loss, employees should regularly back up their SBU folder to a government-owned, encrypted PSD.

4.33.1.6.1
(09-01-2020)

Storing Portable Storage Devices (PSDs)

- (1) Secure sensitive information at all times.
- (2) After data on a PSD is copied to an employee's computer, remove the PSD containing taxpayer, third party, or stakeholder data from the computer and return the PSD to the person who provided it. See IRM 4.33.1.7.1 for instruction on shipping PSD's, which must be adhered to if returning the PSD to the taxpayer, third party, or stakeholder by mail.

Exception: All summoned electronic records must be retained per IRM 25.5.3.6.2.2, Saving Records for Administrative Case File.

Caution: If there is suspicion of fraud, consider retaining the original PSD rather than returning it to the taxpayer, third party, or stakeholder.

- (3) If returning the PSD to the taxpayer, third party, or stakeholder is not possible or if the PSD is retained, the PSD must be stored in a locked container for safeguarding in accordance with IRM 10.8.1.4.10.3, MP-4 Media Storage; IRM 10.2.15, Minimum Protection Standards, for "high security" items; and IRM 10.5.1.6.6, Storage.
- (4) For container security provisions, refer to IRM 10.2.14.3, Containers, and IRM 10.2.14.3.1, Locked Containers.

4.33.1.7
(09-01-2020)

Transmitting Electronic Records

- (1) Electronic data may require transmission to another employee for assistance or conversion from its original format to a readable format (e.g., Excel spreadsheet, PDF, image file). There are several methods that may be used to transmit electronic data.
 - a. **Email** - An approved method for IRS-internal transmission only when encryption is utilized. Do not include SBU data (including PII and tax information) in the email subject line. All email messages containing SBU information are required to be sent encrypted per IRM 10.5.1.6.8(6), Email; IRM 10.5.1.6.8.3, Emails to IRS Accounts; and IRM 11.3.1.17.2, Electronic Mail and Secure Messaging.

Caution: Except as authorized by IRM 10.5.1.6.8.1, Emails to Taxpayers and Representatives, do not send emails to taxpayers or their authorized representatives, even if requested, due to the risk of improper disclosure or exposure per IRM 11.3.1.17.2(7), Electronic Mail and Secure Messaging, and IRM 10.5.1.6.8.1, Emails to Taxpayers and Representatives. For details on email security and encryption, see IRM 10.8.1.4.17.2.2, Electronic Mail (Email) Security.

Note: Electronic accounting data files may be too large to transmit using encrypted email.

Note: Large electronic files may need to be transmitted to the Department of Justice (DOJ) if their assistance is needed in certain matters, e.g. summons enforcement. In such cases, contact Counsel to coordinate a transfer of electronic records to DOJ.

- b. **Instant Message** - An approved secure method; however, transmission of large files may take longer over slower internet connections. Although

it may be used to transmit electronic data files, do not use instant messaging to engage in discussions regarding business decisions related to examinations. See IRM 1.15.6.14.1(5), Use of Agency-approved Electronic Messaging Systems, and IRM 1.15.6.14.2(2) (b) and (c), Preserving Electronic Messages.

Note: When transmitting SBU data files, employees should change the default destination folder (i.e., My Received Files) where transmissions are saved to a sub-folder of the encrypted SBU Data folder (if the instant messaging program allows). Alternatively, the default destination folder can be encrypted by right-clicking on the folder and selecting **Encrypt**.

- c. **Shipping PSDs** - For shipping guidance, see IRM 4.33.1.7.1. One of the alternative methods listed above should be considered in lieu of shipping small PSDs because they can be easily misplaced.

4.33.1.7.1
(09-01-2020)

**Shipping Portable
Storage Devices (PSDs)**

- (1) **Shipping Encrypted PSDs** - PSDs containing SBU data may be shipped if electronic transmittal of the data contained on them is not available or practical. When shipping PSDs with SBU data, the following safeguards must be taken:

- a. Adhere to guidance provided in IRM 10.5.1.6.7.3, Shipping.

Reminder: Monitor the shipment to ensure it is delivered per IRM 10.5.1.6.7.3(21), Shipping. If it is determined a package has been lost, immediately report the loss per IRM 10.5.4.3(1), Reporting Losses, Thefts and Disclosures.

Reminder: Shipping PII through a private delivery carrier requires the use of Form 3210, Document Transmittal. See IRM 4.10.1.4.8, Shipping Personally Identifiable Information (PII).

- b. The files on PSDs must always be encrypted and password protected before they are shipped. See IRM 10.8.1.4.10.4.1, MP-5 Media Transport - Control Enhancements. The current encryption program used by the IRS (e.g., SecureZip, SEERS) should be used to encrypt and password protect electronic records copied to PSDs.

Caution: Insertion of a PSD into an IRS computer automatically copies a Symantec removable media access utility application to the PSD. This access utility application can be used along with a password by a taxpayer or other third party to decrypt the contents on the PSD. Files on the PSD **prior to insertion** are **not** automatically encrypted. See *SEE- Sharing Files with the Access Utility* for additional information.

- c. Never ship passwords with PSDs. Password must be provided verbally or sent separately by mail, email, instant message, or fax.

- (2) **Shipping Unencrypted PSDs** - Never ship unencrypted PSDs containing SBU data. The only exception is when following the *Media Destruction Guidelines* regarding shipping procedures for unencrypted media for final disposition. See IRM 4.33.1.9.1 for additional information on shipping PSDs for final disposition.

4.33.1.8
(09-01-2020)
**Closing Cases with
Electronic Records**

- (1) Electronic information that directly supports an adjustment, penalty, or alternative position, whether obtained voluntarily or through summons procedures, must be printed and included in the paper administrative case file. It must also be included in the RGS case file.
- (2) Electronic records are often large and include many different file types (e.g., accounting software data files). When determining whether to include electronic records that do **not** directly support an adjustment, penalty, or alternative position in the case file, a presumption of retention should be used to prevent deletion of any potentially relevant records. This means that an electronic record must be retained unless it is clear that the record will not be relevant to potential future case activities.

Caution: All summoned electronic records must be retained per IRM 25.5.3.6.2.2, Saving Records for Administrative Case File.

- (3) Do not include accounting software data files in the RGS case file, as they are not compatible with RGS. See IRM 4.10.9.7.11.1, Electronic Accounting Software Backup Data Files and Spreadsheets, for additional information on closing cases with electronic accounting software data files and spreadsheets.
- (4) Retain electronic records in their original format. For example, a document received as a Word file (e.g., docx) must be retained as a Word file. This is necessary to preserve the metadata.
- (5) If electronic records require retention, but they are not compatible with RGS, the original records must be copied to an encrypted PSD and the encrypted PSD must be included with the case file. See IRM 4.10.15.7.19, Office Documents and Case File Documents. Working copies must also be copied to an encrypted PSD and placed in the case file if the working copies add merit or value to support audit adjustments. The decision to include or not include the records in the case file is determined on a case-by-case basis.
- (6) Any SBU data (including PII and tax information) that may need to be safeguarded from unauthorized disclosure before being provided to the taxpayer in a Freedom of Information Act (FOIA) request must be placed in an "To be Opened by Addressee Only" envelope within the case file. Examples might include an informant referral, information regarding fraud potential, third party tax information, etc. This applies to electronic records as well as paper documents. Disclosure personnel will determine if any of the data can be withheld from release in accordance with disclosure guidelines. See IRM 4.10.9.7.3, Workpapers: Disclosure, and IRM 11.3.13.7, Review and Redacting, for additional information.

4.33.1.8.1
(09-01-2020)
**Labeling and Location of
Portable Storage
Devices (PSDs)**

- (1) Each PSD included in a case file must be clearly labeled. On CDs and DVDs, write the following information with a felt tip permanent marker on the top (non-reflective side) of the disk. Do **not** affix a paper label to the CD or DVD. USB storage devices (e.g., thumb drives) are much smaller, so labeling may be taped or affixed rather than written directly on the device. The label must include the following information:
 - Taxpayer name control
 - Last four digits of the taxpayer TIN
 - MFT

- Tax period(s)
- Workpaper number of the PSD (See IRM 4.33.1.8.2).

Note: CDs and DVDs are preferred over USB storage devices for storing electronic records closed with a case file. USB storage devices are more costly and much smaller than CDs and DVDs, resulting in a greater chance of being lost or misplaced.

- (2) If more than one PSD is included in a case file, label each with a number or a unique name. For example, if there are two CDs in a case file, label one CD “1 of 2” and label the other “2 of 2” so when workpapers reference a file on a PSD, the reference clearly points to the relevant PSD.
- (3) Place each PSD in an individual envelope, sleeve, or covering of some type sufficient to protect it from abrasion or damage. The covering must be sealable, clearly state the type of PSD enclosed, and be labeled with the same information in paragraph (1).

Reminder: As stated in IRM 4.33.1.5 (7), passwords should be documented on Lead Sheet 100-1A, External Records Password. Further, per IRM 4.33.1.4.1 (1), passwords must always be stored separately from electronic records.

- (4) Place the envelope, sleeve, or protective covering inside a second envelope. The second envelope must be large enough to hold the first envelope and able to be attached to the inside left of the case folder per IRM 4.10.9.9.2, Forms on the Inside Left of the Case Folder, which also provides the order in which the documents must be assembled.
- (5) Label the outside envelope “Electronic Media.”

4.33.1.8.2
(09-01-2020)
**Referencing Electronic
Files Stored on Portable
Storage Devices (PSDs)**

- (1) All electronic records stored on PSDs in the case file must be referenced by a workpaper to ensure electronic files are easily locatable. See IRM 4.33.1.8 for the type of data that must be saved to a PSD versus stored within RGS.
- (2) Every case that includes a PSD must include a workpaper containing a table of contents for each PSD. See IRM 4.33.1.8.3 for guidance on describing contents of PSDs.

4.33.1.8.3
(09-01-2020)
**Documenting Contents
of Portable Storage
Devices (PSDs)**

- (1) A workpaper containing a table of contents for each PSD must be included in the case file. The workpaper must be printed and documented as a separate issue indexed to Form 4318, Examination Workpapers Index. Refer to *Creating Form 4318-600 Items* for instructions on adding the issue to the RGS case file using a 6XX reference number. If more than one PSD is in the case file, each PSD must be labeled with a unique reference number.

Note: Electronic media will not automatically be returned when requesting prior tax returns and audit files. When the prior tax return and audit file are received, contact the local *AIMS/ERCS staff* if the files have a note attached stating “Electronic media is associated with this return.” The AIMS/ERCS staff will input an ESTAB to request the media by notating “Provide all related electronic media” in the request. See IRM 3.5.61.3.80, Electronic Media.

- (2) The PSD workpaper must include header and footer information as required in IRM 4.10.9.7.1, Workpapers: Headers and Footers, as well as the following information:
 - Identification of disk content (i.e., a listing of each file on the PSD),
 - Media information such as software format (e.g., .xlsx, .pdf, .docx, .qbb), and
 - Type of encryption utilized.
- (3) See IRM 4.33.1.5 (7) for information on where to record passwords for electronic records.

4.33.1.9 (09-01-2020) **Disposing of Electronic Records**

- (1) After all records have been preserved in conformance with applicable requirements and IRM 4.33.1.8, electronic data files that are no longer needed on the examiner's computer hard drive must be deleted. See IRM 4.10.15.7.19(6), Office Documents and Case Files Documents, and IRM 4.10.15.10.1(1), Examined Closures (Forms 1040, 1120, 1120S, 1065, and 1040NR), for information on removing files from RGS.

Caution: Deleting a file from the SBU Data folder does not completely remove it from the hard drive; the recycle bin must also be emptied.

Caution: Agency counsel is responsible for issuing a litigation hold to preserve electronically stored information when litigation is initiated or reasonably anticipated. When invoked, litigation hold procedures override these record retention procedures. See IRM 25.3.1.7, Preserving Electronically Stored Information in Litigation Cases, for additional information on litigation hold procedures and the duty to preserve electronically stored information in litigation cases.

- (2) See IRM 4.33.1.8 and IRM 4.10.9.7.11.1, Electronic Accounting Software Backup Data Files and Spreadsheets, for information on what to do when the data needs to be included in the closed case.

4.33.1.9.1 (09-01-2020) **Disposing of Portable Storage Devices (PSDs)**

- (1) As mentioned in IRM 4.33.1.6.1, all PSDs received from a taxpayer, representative, third party, or stakeholder must be returned, in person, to the individual who provided it after saving the data to the examiner's computer.
- (2) If the examiner is not able to return unneeded media in person:

- a. **Encrypted PSDs** - The PSD can be returned by mail if requested by the taxpayer. See IRM 4.33.1.7.1 (1) for shipping information.

Note: Password protected accounting software data files are considered encrypted media; however, determining whether the data files are password protected cannot be completed until the file is opened by the applicable software.

- b. **Unencrypted PSDs** - Unencrypted media must never be mailed to taxpayers, third parties, or stakeholders (e.g., IRS employees, federal and state agencies) as stated in IRM 4.33.1.7.1 (2). Employees are responsible for protecting any SBU information they may have in their possession, whether the SBU is in paper form or on IRS computer equipment and computer systems. Sensitive information and SBU that is

stored or transmitted by computer equipment (such as laptops and portable storage devices) must always be encrypted.

- (3) If the taxpayer is no longer available, doesn't want the records returned, or returning the PSD is not feasible, the media (both encrypted and unencrypted) must be disposed of in accordance with *IT Media Destruction procedures*.