DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

SMALL BUSINESS/SELF-EMPLOYED DIVISION

Date: 03-13-2026

Control Number: SBSE-04-0326-0029
Expiration Date: 03-13-2028
Affected IRM(s): 4.10.1 and 4.33.1

MEMORANDUM FOR AREA DIRECTORS, FIELD EXAMINATION AND SPECIALTY

FROM: Heather J. Yocum /s/ *Heather J. Yocum*
Director, Examination Field and Campus Policy
Acting Director, Specialty Examination Policy

SUBJECT: Revised Supplemental Guidance on Offering Digital Communication Tools to Taxpayers and Third Parties

This memorandum supersedes the interim guidance in SBSE-04-0126-0013.

Purpose: The purpose of this memorandum is to incorporate changes from the guidance in IGM SBSE-04-0126-0012, *Interim Guidance on Offering Digital Communication Tools to Taxpayers and Third Parties*, into IRM 4.10.1, *Examination of Returns, Overview of Examiner Responsibilities*, and IRM 4.33.1, *Managing Electronic Records from Taxpayers and Third Parties*, until they are published. Please ensure this information is distributed to all affected employees in your organization.

Effect on Other Documents and Effective Date: This guidance in SBSE-04-0126-0012, *Interim Guidance on Offering Digital Communication Tools to Taxpayers and Third Parties*, will be incorporated into IRM 4.10.1, *Overview of Examiner Responsibilities*, and IRM 4.33.1, *Managing Electronic Records from Taxpayers and Third Parties*, by a date not to exceed two years from the date of this memorandum. The following changes are effective 03/13/2026.

Contact: Ronald Zarriello, Program Manager, Examination Field and Campus Policy, Field Examination General Processes.

Attachment:
Attachment 1 – IRM 4.10.1
Attachment 2 – IRM 4.33.1

Distribution: www.irs.gov

Attachment 1, IRM 4.10.1

IRM 4.10.1.1.5
Terms

(1) The following table defines the key terms used throughout this IRM.

Term	Definition
Authorized user	An individual designated by a taxpayer to access and use Taxpayer Digital Communications (TDC) Secure Messaging (SM) on their behalf. The IRS must have a valid Form 2848 or Form 8821 on file to substantiate the individual's authority to exchange information on behalf of the taxpayer.
Data Protection	[No changes]
Digital Signature	[No changes]
Digital Communication Tool	A web-based system that allows electronic communication between two parties. Note that only certain digital communication tools (e.g., Document Upload Tool for Taxpayer Facing Employees (DUT-TPFE), Taxpayer Digital Communications (TDC) Secure Messaging (SM), etc.) are approved for use between certain examiners and an external party (i.e., a taxpayer, representative, or third party).
Document Upload Tool for Taxpayer Facing Employees (DUT-TPFE)	An IT-approved, one-way (taxpayer to examiner), digital communication tool that taxpayers and third parties can use to submit documents and information related to compliance interactions.
E-fax	[No changes]
EEFax (Enterprise e-Fax)	[No changes]
Electronic Signature	[No changes]
Embedded Quality (EQ)	[No changes]
Embedded Quality Review System (EQRS)	[No changes]
Knowledge Base Articles (KBAs)	Standard language that can be added to Taxpayer Digital Communications (TDC) Secure Messaging (SM) messages sent to the taxpayer and their authorized users. Other than ministerial messages discussed in IRM 4.10.1.1.3.2.1, all messages sent to the taxpayer or their authorized users must either (1) consist solely of content from one of the KBAs or (2) be approved by the examiner's manager per IRM 4.10.1.3.2(4), *Written Communication*.
Ministerial Message	[No changes]
National Quality Review System (NQRS)	[No changes]
Personally Identifiable Information (PII)	[No changes]
Personal	[No changes]

Identification (PID) Number	
Pocket Commission	[No changes]
Pseudonym	[No changes]
Repository	[No changes]
Standard Employee Identifier (SEID)	[No changes]
SmartID Card	[No changes]
Taxpayer Digital Communications (TDC) Secure Messaging (SM)	An IT-approved, two-way, digital communication tool that provides employees and taxpayers (and their authorized users) a way to send and receive written text and attachments electronically through a secure portal.
Work Plan	[No changes]

IRM 4.10.1.3.2
Written Communication

(1) All correspondence must contain the name of the person to contact (examiner or group manager depending on the type of letter), telephone number, personal identification number, and a signature. See IRM 4.10.1.2.2.2, *Employee Contact Information*, for guidance.

> **Note:** If the taxpayer's SSN or EIN is displayed on correspondence, it must show only the last four digits.
>
> **Exception**: For SB/SE, Knowledge Base Articles (KBAs) sent through TDC SM do not need to contain a signature since the examiner's name automatically populates in the text of the secure message body. However, the examiner's signature is required on **attached** forms and letters that have signature lines.

(2) When possible, all correspondence with taxpayers should be prepared using approved form letters, since the specific language in these documents has been approved for general public use. System-generated (e.g., RGS, IMS, etc.) letters should be used when the most current version of the letter is available within the system.

> **Note:** Examiners must not modify the approved forms and letters.
>
> **Note:** For SB/SE, when corresponding with the taxpayer and their authorized users through TDC SM, examiners must use KBAs when available and appropriate. If an appropriate KBA does not exist and a message sent to the taxpayer/authorized user(s) is not ministerial (as discussed in IRM 4.10.1.3.2.1), examiners must obtain managerial approval to send the message per IRM 4.10.1.3.2(4).

(3) [No Changes]

(4) [No Changes]

(5) [No Changes]

IRM 4.10.1.3.2.1
Ministerial Messages

(1) [No Changes]

(2) [No Changes]

(3) [No Changes]

(4) Ministerial messages may be sent via TDC SM.

Note: Because TDC SM is a secure portal, SBU may be included in the subject line. Therefore, examiners should ensure the subject line of outgoing TDC SM messages reflects the nature of the message.

IRM 4.10.1.3.3
Written Communication to the Taxpayer's Representative

(1) [No Changes]

(2) Examiners are required to prepare and send Letter 937, *Transmittal Letter for Power of Attorney*, to the power of attorney (POA) to transmit copies of correspondence addressed to the taxpayer.

Exception: For SB/SE, Letter 937 is **not** required when sending messages and/or attachments to the representative in TDC SM if the taxpayer is **also** registered in TDC SM and the representative is included in the 'copies to'/'copy to emails' field of the taxpayer's TDC SM case.

(3) Copies of letters and other forms and documents addressed or specific to the taxpayer should be enclosed with Letter 937, *Transmittal Letter for Power of Attorney*, and sent to the representative at the same time they are sent to the taxpayer. Examples of other forms and documents addressed or specific to the taxpayer include but are not limited to Form 4564, *Information Document Request*; Form 872, *Consent to Extend the Time to Assess Tax*; Form 4549, *Report of Income Tax Examination Changes*, etc.

Note: The enclosure section of Letter 937 should indicate the specific enclosures included with Letter 937. For example, if Letter 3572, *SB/SE Office Exam Call-Back Appointment Letter*, is enclosed with Letter 937, the examiner should check the "Letter(s)" box and type "3572" in the fillable field.

Note: When a representative communicates with the examiner electronically (for example, using TDC SM) but the taxpayer chooses not to, the taxpayer must be timely furnished copies of **all** formal correspondence and attachments (e.g., form letters and enclosures) that were sent to the representative electronically. Such copies must be sent to the taxpayer using an approved communication method. The examiner must document the activity record with the date and method of transmission.

IRM 4.10.1.X
Use of Digital Communication Tools in Taxpayer and Third-Party Interactions (SB/SE Only)

(1) Taxpayers and third parties may submit documentation or information related to compliance inquiries and interactions via IT-approved digital communication tools (e.g., DUT-TPFE, TDC SM, etc.) unless there is a specific prohibition.

(2) The use of IT-approved digital communication tools is voluntary for taxpayers.

(3) Examiners are required to offer and encourage the use of IT-approved digital communication tools to taxpayers and third parties during compliance interactions and must document they were offered in the case history (e.g., Form 9984, Examining Officer's Activity Record, etc.).

Note: Most tools require BEARS entitlements. However, access to specific digital communication tools depends on whether the examiner's business unit or function is approved to utilize the tool. As a result, examiners may not have access to every digital communication tool. For more information on tool availability, visit Emerging Technologies - Home.

(4) Correspondence and documents received via IT-approved digital communication tools generally must be saved to an encrypted folder on the examiner's hard drive or OneDrive upon receipt. See IRM 4.33.1.4(2), *Accessing Electronic Records*, and IRM 1.15.6.8(3)(d), *Creation, Use, and Maintenance of Unstructured Electronic Data*, (related to the use of OneDrive for the temporary storage of Federal records).

Note: Documents received and temporarily saved on the examiner's hard drive or OneDrive must be associated with the case file when appropriate. See IRM 4.33.1.8, *Closing Cases with Electronic Records,* for guidance on preserving all appropriate documents in the electronic case file.

(5) See IRM 10.10.1.6.1, *Accepting Images of Signatures and Digital Signatures in Certain Taxpayer Interactions*, for guidance on accepting **signed** documentation via digital communication tools.

(6) Correspondence received via a digital communication tool falls under the activity "Response to correspondence" in IRM Exhibit 4.2.8-1, *National Standard Time Frames for Case Action*, and requires action within 14 calendar days of receipt.

Attachment 2, IRM 4.33.1

IRM 4.33.1.3
Receiving Electronic Records

(1) [No Changes]

(2) Taxpayers and their representatives provide electronic records by:

a. **Email** – Employees must advise taxpayers and their representatives that the IRS 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(4), *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.

c. **Document Upload Tool for Taxpayer Facing Employees (DUT-TPFE) –** Employees with access to DUT-TPFE may receive records from taxpayers and third parties by DUT-TPFE unless there is a specific prohibition. See SB/SE Exam – DUT-TPFE FAQs for additional information on DUT-TPFE.

d. **Taxpayer Digital Communications (TDC) Secure messaging (SM)** – Employees with access to TDC-SM may receive records from taxpayers by TDC SM unless there is a specific prohibition. See SB/SE Field Examination TDC SM User Guide and TDC SM FAQs for additional information on TDC SM.

e. 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* book and the *Sources that Respond Electronically* page for approved electronic summons processes.

IRM 4.33.1.4
Accessing Electronic Records

(1) Examiners must complete the following actions when electronic records are received on a PSD:
   a. Perform a virus scan in a standalone environment as required in IRM 10.8.1.4.19.2(9), *SI-03 Malicious Code Protection*. For step-by-step instructions, see the *How to Run a Virus Scan* page. Document virus scan actions in the case history (e.g., Form 9984, *Examining Officer's Activity Record*, etc.).

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 the *IRS Computer*

Security Incident Reporting Procedures.

b. Save the files to an encrypted folder on the examiner's computer or OneDrive. (See IRM 1.15.6.8(3)(d), *Creation, Use, and Maintenance of Unstructured Electronic Data*, related to the use of OneDrive for the temporary storage of Federal records). If it is not possible to immediately save the information, it must be done at the earliest opportunity.

   Note: If it's immediately apparent that the files received should be associated with the case file (e.g., a signed Form 4549, Form 872, etc.), the examiner should save the files directly to the electronic case upon receipt (bypassing the need to save the files to an encrypted folder on the examiner's computer or OneDrive). As discussed in IRM 4.33.1.8, the decision to include or not include electronic records in the case file is determined on a case-by-case basis.

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 or a digital communication tool**:

a. Save the files to an encrypted folder on the examiner's computer or OneDrive. (See IRM 1.15.6.8(3)(d), *Creation, Use, and Maintenance of Unstructured Electronic Data*, related to the use of OneDrive for the temporary storage of Federal records). If it is not possible to immediately save the information, it must be done at the earliest opportunity.

   Note: If it's immediately apparent that the files received should be associated with the case file (e.g., a signed Form 4549, Form 872, etc.), the examiner should save the files directly to the electronic case upon receipt (bypassing the need to save the files to an encrypted folder on the examiner's computer or OneDrive). As discussed in IRM 4.33.1.8, the decision to include or not include electronic records in the case file is determined on a case-by-case basis.

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 should I contact for assistance?*.

(4) [No Changes]

IRM 4.33.1.5
Preserving Original Records and Creating Working Copies

(1) Examiners must document all actions regarding electronic records in the case history (e.g., Form 9984, *Examining Officer's Activity Record*, etc.) 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, digital communication tool, etc.).
- 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 1.15.6.12, *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 saved in 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 in the appropriate recordkeeping system. 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, OneDrive, or the electronic case file 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) [No Changes]

(7) For PSDs stored in physical (i.e., paper) case files , examiners should record user names and passwords for all PSDs on Lead Sheet 100-1A, *External Records Password* (or equivalent). 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, *Application and Operating System (OS) Password Policies for Non-MFA Systems*.

(8) [No Changes]

IRM 4.33.1.6
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 in an encrypted folder on the examiner's hard drive, on OneDrive, or in the electronic case file until they are no longer needed. See IRM 4.33.1.8 for guidance on when to include electronic files with the closed case file.

Exception: Electronic records may be maintained on an encrypted PSD for certain cases. Taxpayer data on PSDs (in physical (i.e., paper) case files) 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(2), *Encryption*. See IRM 4.33.1.5(7) for guidance on recording and storing passwords. See IRM 1.15.6.8(3)(f), *Removable Media*, for additional information on properly storing removable media.

[paragraph 2 was revised and incorporated into paragraph 1]

(2) [Formerly paragraph 3; revised] Sensitive But Unclassified (SBU) data on the employee's hard drive must always be in an encrypted folder.

[Paragraph 4 deleted]

IRM 4.33.1.8
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 included in the case file. For SB/SE Field Examination, see IRM 4.10.9.6(3), *Overview of Lead Sheets and Workpapers.*

(2) [No Changes]

(3) Accounting software data files may require special handling in electronic cases. For example, see IRM 4.10.9.8.9, *Accounting Software Backup Data Files and Spreadsheets*, for additional information on closing cases with electronic accounting software data files and spreadsheets in RGS.

(4) [No Changes]

(5) If electronic records require retention, but they are not compatible with the recordkeeping system, the original records may require special handling (e.g., for RGS, see *What files are not compatible with RGS?* and IRM 4.10.15.10(3), *Office Documents (OD) and Case File Documents (CFD)*). Working copies must also be included 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) See IRM 4.10.9.8.3.1, *Extremely Sensitive Information*, for guidance on the proper use of Other Gov TD F 15-05.11, *Sensitive But Unclassified (SBU) Cover Sheet*, with extremely sensitive information in the case file.

IRM 4.33.1.9
Disposing of Storing 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 or OneDrive must be deleted. (For case files in RGS, see IRM 4.10.15.10(5), *Office Documents (OD) and Case Files Documents (CFD)*, for information on removing files.)

Caution: Deleting a file from the computer hard drive or OneDrive does not completely remove it; 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.