IRM PROCEDURAL UPDATE

DATE: 01/26/2026

NUMBER: 4.23.3

SUBJECT: Instruction and Guidance to Examiners for the Mandatory Offering of IT-Approved Digital Communication Tools

AFFECTED IRM(s)/SUBSECTION(s): 4.23.3

CHANGE(s):

IRM 4.23.3.8.4(10) - New paragraph (10) was developed to inform examiners that it is mandatory to offer the taxpayer the use IT-Approved digital communication tools.

(10) The examiner is to offer the taxpayer and their representative the use of a digital communication method to correspond and exchange information after initial contact. Employees are to use IT-Approved digital communication tools to facilitate effective and efficient digital communications.

IRM 4.23.3.9 - Inserting a new subsection titled "Digital Communication Tools." This subsection will incorporate instruction and guidance to examiners for the use of IT-Approved digital communication tools into their compliance work.

(1) A digital communication tool is a web-based system that allows electronic communication between two parties. An examiner is required to offer and encourage the use of IT-approved digital communication tools with taxpayers and representatives during compliance interactions . Examples of IT-approved digital communication tools are Document Upload Tool for Taxpayer Facing Employees (DUT-TPFE) and Taxpayer Digital Communications (TDC) Secure Messaging (SM), etc. Refer to IRM 10.5.1.6.8.6, *Other Secure Electronic Communication Methods*.

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 them. As a result, examiners may not have access to every digital communication tool. For more information on tool availability, visit Emerging Technologies Knowledge Base Homepage.

Note: Taxpayers and representatives are not required to submit any documentation or information via IT-approved digital communication tools. They may continue to submit information by mail or other allowable means of transmission.

(2) Taxpayer submissions of documentation, forms, letters, and returns related to post-filing/non-filing inquiries and interactions can be allowed using digital communication tools, unless there is a specific prohibition.

(3) IRS employees are required to protect the privacy of sensitive but unclassified (SBU) data for taxpayers and personnel, including personally identifiable information (PII), such as federal tax information (FTI), tax return, financial, and employment information regardless of format. Refer to IRM 10.5.1, *Privacy Policy*.

(4) The examiner should explain the IT-approved digital communication tools available to help the taxpayer determine which option makes the most sense for their circumstances (depending on the frequency of use, file type(s)/size(s), etc.).

IRM 4.23.3.9.1 - Inserting a new subsection titled "Sending Records via IT-Approved Digital Communication Tools." This subsection will incorporate instruction and guidance to examiners for sending communication through IT-Approved digital communication tools into their compliance work.

(1) 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 (for example, RGS, IMS, etc.) letters should be used when the most current version of the letter is available within the system. See IRM 4.10.1.3.2, *Written Communication*.

Reminder: If the taxpayer's SSN or EIN is displayed on correspondence, it must be redacted to show only the last four digits.

Note: If an appropriate correspondence does not exist and the message is not ministerial (as discussed in IRM 4.10.1.3.2.1, *Ministerial Messages*), examiners must obtain managerial approval to send the message per IRM 4.10.1.3.2 (4).

(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. Refer to IRM 4.10.1.3.3, *Written Communication to the Taxpayer's Representative*.

Exception: SB/SE employees Letter 937 is not required when sending messages and/or attachments to the representative in Taxpayer Digital Communications (TDC) Secure Messaging (SM) application 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) Examiners must not send emails that include SBU data (including PII and tax information) to taxpayers or their authorized representatives, even if requested, because of

the risk of improper disclosure or exposure. See IRM 10.5.1.6.8.1, *Emails to Taxpayers and Representatives*, for further information and limited exceptions.

IRM 4.23.3.9.2 - Inserting a new subsection titled "Receiving Records via Digital Communication Tools." Incorporate instruction and guidance to examiners for receiving communication through IT-Approved digital communication tools into their compliance work.

(1) Taxpayer submissions of documentation, forms, letters, and returns related to post-filing/non-filing inquiries and interactions are to be allowed through digital communication tools unless there is a specific prohibition.

Reminder: Necessary precautions are to be taken to safeguard the data, IRS computers, and the IRS network.

Caution: Careful consideration should be given to accepting image of return information in conjunction with examination activity. Examiners must evaluate the need to examine original documents as opposed to images of documents.

(2) 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.

(3) 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, *Accessing Electronic Records*, paragraph (2) andIRM 1.15.6.8 (3)(d), *Creation, Use, and Maintenance of Unstructured Electronic Data*, paragraph (3) item (d) (related to the use of OneDrive for the temporary storage of Federal records).

Note: Documents received from the taxpayer and temporarily saved on the examiner's hard drive or OneDrive must be associated with the IMS 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.

(4) If it is immediately apparent that digital received files should be associated with the case file (for example, a signed Form 2504, Form SS-10, etc.), the examiner should save the files directly to the IMS 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.

Note: Requirements to incorporate the documents received into your case file review IRM 4.23.4, *General Procedures and Workpapers* and IRM 4.23.10.19, *Assembly of Employment Tax Case*.

(5) Taxpayers and their representatives may provide electronic records by these methods:

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 further information see IRM 10.5.1.6.8.1, *Emails to Taxpayers and Representatives*, and IRM 4.33.1.4, *Accessing Electronic Records,* paragraph (2).

   Note: See IRM 10.5.1.6.8.1 for guidance when an examiner receives an unsolicited email from a taxpayer or tax professional.

   Note: For sending external (outside the IRS network) electronic communication it is strongly recommended employees use IRS secure alternatives to email. For the use of IRS email accounts see IRM 10.5.1.6.8.6, *Email and Other Electronic Communications*, and its subsections.

b. **Portable Storage Device (PSD)** – When electronic records are received on a PSD, employees must follow procedures to protect IRS computers and the IRS network before accessing the records. See IRM 4.33.1.4 paragraph (1) for guidance on accessing records stored on PSDs.

(6) See IRM 4.33.1.9, *Disposing of Storing Electronic Records* for guidance on removing digital documents obtained from a taxpayer that were temporarily stored on an employee's hard drive or OneDrive folder.