TAXPAYER ADVOCATE SERVICE
YOUR VOICE AT THE IRS

OFFICE OF THE TAXPAYER ADVOCATE
WASHINGTON, DC 20224

December 6, 2021

Control No: TAS-13-1221-0015
Expires: 10/31/2023
Impacted IRMs: 13.1.24, IRM 13.1.6

MEMORANDUM FOR TAXPAYER ADVOCATE SERVICE EMPLOYEES

FROM: /s/ Bonnie Fuentes
Executive Director Case Advocacy, Intake and Technical Support

SUBJECT: Interim Guidance – Digital Signatures and External Email Communications

This memorandum supersedes the May 17, 2021 memorandum (TAS-13-0521-0007) with an extended expiration date.

As part of TAS's continuing response to the COVID-19 situation, we are taking additional steps to protect our employees while strongly advocating on behalf of taxpayers. We are maximizing our ability to share and receive information in remote working environments where employees, taxpayers, and their authorized third parties are working from alternate locations.

This memorandum generally mirrors the guidance provided on these same topics discussed in the Memorandum for All Services and Enforcement Employees, (1) Approval to Accept Images of Signatures and Digital Signatures (2) Approval to Receive Documents and Transmit Encrypted Documents by Email, dated November 18, 2021, by Douglas W. O'Donnell, Deputy Commissioner, Services and Enforcement.

Pursuant to IRM 1.11.2.2.4, When Procedures Deviate from the IRM, we are extending a temporary deviation that allows TAS employees the ability to receive and transmit documents by email to taxpayers and authorized third parties with their consent using password-protected encrypted attachments and to accept images of signatures (scanned or photographed) and digital signatures on certain IRS and TAS documents when no other approved electronic alternative is available.

TAS employees have the option to use their assigned IRS email address to send or receive emails from taxpayers or authorized third parties. Employees who do not wish to use this option will discuss with their manager the available alternatives (*e.g.*, manager, analysts or secretary emailing documents on employee's behalf). TAS employees are prohibited from using their personal email addresses for communicating with taxpayers or their authorized third parties.

Using Email to Send Letters and Other Documents to Taxpayers and Authorized Third Parties

With the taxpayer or representative's consent, TAS employees may use email to transmit letters and other documents to the taxpayer or representative using password-protected encrypted attachments. TAS employees will inform taxpayers or authorized third parties that they may have to purchase software to access the attachments to the email. This guidance only extends to the taxpayer and his or her authorized representative(s). Employees must not email third-party contacts.

NOTE: An initial contact with a taxpayer or representative must never be made by email. The decision to send or receive documents by email is at the discretion of the taxpayer and should only be used if the taxpayer or representative is unable to use another approved electronic alternative.

When sending an encrypted attachment, TAS employees must take the following steps:

1. Make sure the taxpayer (or representative) has already been authenticated pursuant to IRM 13.1.16.4.1, Disclosure and IRM 11.3.2.3.2, Requirements for Verbal or Electronic Requests. In addition, verbally verify the recipient's email address. If interacting with a Congressional Office, be sure there is a waiver from the taxpayer and that you have properly authenticated the contact from the Congressional office. *See* IRM 13.1.16.8.7, Congressional Office Contacts.
2. Obtain the taxpayer or representative's consent to transmit encrypted documents by email. See Step 4 below. Employees must not email taxpayers or authorized third parties unless they have provided consent to receive email. Follow applicable guidance to ensure that the person providing consent is authorized to do so, particularly if multiple individuals are involved.
3. Create a password that is 12 characters, include upper and lower-case letters, a symbol, and a number. Share this password with the taxpayer, representative, or Congressional office. If the taxpayer has given TAS permission to leave information on voicemail per IRM 13.1.6.7(3), Leaving Messages on Answering Machines, and TAS is unable to reach the taxpayer, TAS will provide the password in a voicemail message. TAS cannot leave tax information on the answering machine or voicemail of the taxpayer's authorized representative or Congressional office. See IRM 13.1.6.7(8). Inform the taxpayer or authorized representative that this password will be used throughout the life of the case if the Case Advocate needs to send documents via email, unless the taxpayer or third party informs you that his or her email has been comprised or requests a new password. Record the password in TAMIS. **Create a new password for each taxpayer or authorized third party.** (Example: Advoc@te4Me!) Don't use the same password for different cases, and don't share the password with other individuals who don't have a business need to know.

4. Employees must obtain consent initially and preserve it as documentation. Advise the taxpayer or representative that consent is only valid for the life of the current TAS case and that he or she may revoke this consent at any time. Ask the taxpayer or authorized third party to send you a test email to confirm the email address and provide the following statement of consent: "[I, [name of the taxpayer or representative], consent to receive encrypted documents by email from [employee name] and associated IRS personnel for the duration of the current TAS case."
5. Inform the taxpayer or authorized third party by phone call that you will be transmitting the document through a password-protected encrypted attachment.
6. **Keep all sensitive information out of the subject line and body of emails (*e.g.*, taxpayer name, last four digits of the taxpayer's TIN, taxpayer's name control, etc.). Exclude identifying information for the name(s) of the attached file(s) as well.** Instead use password protected encrypted attachments. Do not include case discussions in the body of the email; rather this discussion will take place in the letter sent as a password protected encrypted attachment.
7. Transmit the documents using the instructions in Attachment 1, Encryption of Outgoing Email Attachments. Employees will copy (CC) another TAS employee such as the office secretary, analyst, or manager on emails sent to taxpayers or authorized third parties. This will ensure the case can move forward in the event that you are unexpectedly on leave. Explain to the taxpayer or authorized third party why you are including a CC on the email.
8. Document the actions performed in the TAMIS History and attach a copy of the email to TAMIS.

Important Reminder: Employees must use the instructions above to send an encrypted email attachment to taxpayers or authorized third parties. Failure to do so may result in an attempted unsecured email transmission that will be blocked by the Safeguarding Personally Identifiable Information Data Extracts (SPIIDE) Automated Data Loss Prevention (DLP) Tool. Incident Management may receive SPIIDE events for investigation and will address within established procedures, when received.

Caution: Do not use the body of the email message, with or without attachments, to discuss the status of the case or request documents or information from the taxpayer or authorized third party. Doing so increases the risk of the email being blocked by the SPIIDE Automated DLP Tool. All discussions about the case or requests for information or documents will be made using a letter to the taxpayer or representative and sent as an encrypted email attachment.

Managers will discuss these procedures with their employees prior to their initial use, to answer any questions and ensure their employees understand the steps that must be performed. If you have questions on how to perform these procedures contact the Business Modernization hotline at 888-331-8226, access code 9600761.

Receiving Documents Electronically from Taxpayers and their Authorized Third Parties

The choice to transmit documents electronically is solely that of the taxpayer. If the taxpayer is not able to eFax the executed document, the taxpayer may use email with attachments to transmit the document to TAS if the following steps are taken:

1. Make sure the taxpayer or representative has already been authenticated pursuant to IRM 13.1.16.4.1, Disclosure. In addition, verbally verify the email address. If interacting with a Congressional Office, be sure there is a waiver from the taxpayer and that you have properly authenticated the contact from the Congressional office. *See* IRM 13.1.16.8.7, Congressional Office Contacts.
2. Advise the taxpayer or authorized third party by phone that communications via unencrypted email over the internet are not secure. Explain that, except for minimal identifying information in the body of the email (*e.g.*, last name, TAMIS case file number), they should keep sensitive information out of the subject line and body of emails and should use password-protected encrypted attachments as much as possible. The document must be in one of the file types specified in Attachment 1.
3. Remind taxpayers or authorized third parties to use strong passwords for encrypting files (at least twelve characters, including a mix of upper- and lower-case letters, numbers, and special characters).
4. Direct taxpayers or authorized third parties to the User Guide at IRS.gov/UsingEmail for additional information about encrypting files and sending documents to TAS by email.
5. As discussed below, if the document contains a signature, the taxpayer or authorized third party must include a statement, either in the form of an attached cover letter or within the body of the email to the effect, "The attached document includes [name of taxpayer]'s valid signature and the taxpayer intends to transmit the attached document to the TAS." If a taxpayer fails to include this statement, request it in a follow-up telephone call. If the TAS employee is unable to secure a statement from the taxpayer, TAS will accept the documentation provided by the taxpayer or authorized third party and document the attempts in the TAMIS history. **Retransmitting attachments is not required.**
6. After you receive the document via email, document step 2 in TAMIS and attach the document(s) and the email or cover letter, as appropriate, in TAMIS.

Caution: Beware of unsolicited emails and email attachments. Do not open any attachments when you were not expecting the taxpayer or authorized third party to send you documentation. Double check to be certain the email address on the email is the same as the address provided by the taxpayer or authorized third party. When in doubt, contact the taxpayer or authorized third party to verify authenticity before opening an attachment.

Accepting Official IRS and TAS Documents with Digital Signatures

The IRS has temporarily agreed to accept digital signatures on certain documents submitted by taxpayers. As such, TAS employees may accept images of signatures (scanned or photographed)

and digital signatures on the following IRS and TAS official documents when advocating for our taxpayers:

- Documents used in the determination or collection of tax liability that will be provided to a Business Operating Division or function such as an attachment to an Operations Assistance Request, including the following:
  - extensions of statutes of limitations on assessment or collection, agreements to extend the time to bring suit, waivers of statutory notices of deficiency and consents to assessment,
  - agreements to specific tax matters or tax liabilities (closing agreements),
  - prior-year (delinquent) tax returns secured through an examination or collection interaction,

  Caution: Returns which are not yet due to be filed, including extensions, should be filed in accordance with instructions for the respective form.

  Reminder: TAS employees should **not** solicit returns from taxpayers as TAS offices are not proper filing locations, and TAS employees are not authorized to accept hand-carried returns. See IRM 13.1.18.8.3, Taxpayers Delivering Returns to TAS and TAS Date Stamp.
  - other statements or forms needing the signature of a taxpayer or representative traditionally collected by IRS personnel outside of standard filing procedures, and
  - other statements or documents relevant to development of a case, not limited to IRS forms or signed documents.
- Form 911, Request for Taxpayer Advocate Service Assistance (And Application for Taxpayer Assistance Order); and
- Written authorization for disclosure signed by a taxpayer and submitted to TAS by Congressional Offices in accordance with IRM 13.1.8.8, Disclosure Issues.

Note: IRS has provided two digital alternatives for submitting third-party authorizations (Forms 2848 and 8821), Submit Forms 2848 and 8821 Online and Tax Pro Account. Tax professionals should be encouraged to use these applications to the extent possible. If a tax professional indicates they are unable to use these options, you may accept case-specific authorization forms by password-protected encrypted email.

Caution: Documents that contain a notice required by law (*e.g.*, notice of third-party contacts under IRC § 7602(c)(1), a notice of deficiency under IRC § 6212, etc.) must be delivered by the means, if any, prescribed by the applicable legal authority.

TAS will accept images of signatures (scanned or photographed) in any of the common file type such as tiff, jpg, jpeg, pdf, etc. In addition, TAS will also accept Digital Signatures that use encryption techniques that provide proof of original and unmodified documentation when transmitted by an approved secure messaging or file transfer system or by email as described in

Receiving Documents Electronically from Taxpayers, above. If a taxpayer or authorized third party does not have this capability, the employee may suggest the use of an imaged signature.

Use of eFax

EFax is still the preferred method of receiving documents from taxpayers or authorized third parties who have the ability to fax, because the transmissions are secure and received electronically as an email. However, employees will not use the underlying email address associated with an eFax to securely email back and forth with a taxpayer or authorized third party. Instead employees will use their individually assigned email address when choosing to send an email to a taxpayer or authorized third party using the procedures discussed above.

Records Management

Records created through electronic interactions with taxpayers are subject to the records management guidance in IRM 1.15, including IRM 1.15.6, Managing Electronic Records.

Incident Reporting

Immediately report incidents. To report data loss, inadvertent disclosure, or other incidents pertaining to these flexibilities, refer to the procedures secribed in IRM 10.5.4.3, Reporting Losses, Thefts and Disclosures. You can also refer to the If/Then Guide for Reporting Incidents and Data Breaches for reporting requirements for specific types of incidents.

TAS employees may use this temporary digital signature and email guidance until October 31, 2023. At the end of this period, the NTA will reevaluate if circumstances warrant extending the time for the continued acceptance of digital signatures and/or use of email to communicate with taxpayers or authorized third parties.

Effect on Other Documents: This IGM supersedes IGM TAS-13-0521-0007 issued May 17, 2021. This IGM supplements IGM TAS-13-0320-0006 and IGM TAS-13-0320-0008. TAS may incorporate this guidance into the next revision of IRM 13.1.24, Advocating for Case Resolution and IRM 13.1.6, Casework Communications.

Please contact Michael Kenyon, Deputy Executive Director of Case Advocacy, Technical Support, at (701) 237-8299, if you have questions.

www.irs.gov