TAXPAYER ADVOCATE SERVICE

YOUR VOICE AT THE IRS

THE OFFICE OF THE TAXPAYER ADVOCATE OPERATES INDEPENDENTLY OF ANY OTHER IRS OFFICE AND REPORTS DIRECTLY TO CONGRESS THROUGH THE NATIONAL TAXPAYER ADVOCATE.

July 8, 2020

Control No: TAS-13-0720-0014
Expires: 12/31/2020
Impacted IRM(s): 13.1.24

MEMORANDUM FOR TAXPAYER ADVOCATE SERVICE EMPLOYEES

FROM: /s/ Bridget Roberts
Deputy National Taxpayer Advocate

SUBJECT: Interim Guidance – Digital Signatures and External Email Communications

This memorandum supersedes the April 13, 2020 memorandum (TAS-0420-0009) with an extended expiration date and additional information on encryption technologies.

As part of TAS's continuing response to the COVID-19 crisis, we are taking additional steps to protect our employees while still 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 representatives 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 June 12, 2020, by Sunita Lough, Deputy Commissioner, Services and Enforcement.

Pursuant to IRM 1.11.2.2.4, *When Procedures Deviate from the IRM*, we are implementing a temporary deviation that allows TAS employees the ability to receive documents by email, transmit documents via email to taxpayers and representatives with their consent using password-protected encrypted attachments via SecureZip or other encryption methods discussed below, and to accept images of signatures and digital signatures on IRS and TAS documents. TAS employees will first use all existing and previously allowable means of receiving and transmitting documents, such as, mail or eFax. However, if an employee's office is unable to receive or send mail or the

taxpayer or representative does not have the ability to fax documents or send mail, the documents can be sent, received and accepted using the procedures discussed in this memorandum.

TAS employees have the option to use their assigned IRS email address to send or receive emails from taxpayers or representatives when mail or fax are unavailable. 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 representatives.

Using Email to Send Letters and Other Documents to Taxpayers and Representatives

If necessary and ***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 via SecureZip or other encryption methods discussed below. TAS employees will inform taxpayers or representatives that he or she may have to purchase software to access the attachments to the email.

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

1. Make sure the taxpayer (or representative (including Congressional Offices)) has already been authenticated pursuant to IRM 13.1.16.2.1, *Disclosure*. In addition, verbally verify the recipient's email address.
2. Create a password that is 12 characters, include upper and lower-case letters, a symbol, and a number. Share this password with the taxpayer or representative during the initial telephone call in Step 1 above. Inform the taxpayer 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 representative 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 representative.** (Example: Advoc@te4Me!) Don't use the same password for different cases, and don't share the password with other individuals that don't have a business need to know it.
3. To reduce issues with taxpayers or representatives opening the file, change the Passphrase Type to "Traditional." This link provides tips on setting a Passphrase Type.
4. Ask the taxpayer or representative to send you a test email to confirm the

email address, with a statement indicating “[Name of taxpayer or representative] consents to receiving documents by SecureZip.”

5. Inform the taxpayer or representative by phone call that you will be transmitting the document through a password-protected SecureZip attachment.
6. **Keep sensitive information out of the subject line and body of emails**; 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 SecureZip attachment.
7. Transmit the documents using the instructions provided by Information Technology and the password discussed in Step 2 above. Employees will copy (CC) another TAS employee such as the office secretary, analyst, or manager on emails sent to taxpayers or representatives. This will ensure the case can move forward in the event that you are unexpectedly on leave. Explain to the taxpayer or representative why you are including a CC on the email.
8. If you did not previously share the password with the taxpayer in Step 2, inform the taxpayer or representative of this password via telephone. 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. See IRM 13.1.6.7(8). As a last resort, if the employee is unable to contact the taxpayer via phone or leave a voicemail, send the password in a separate email. **Do not transmit the password in the same email as the documents.**
9. Document the actions performed in the TAMIS History and attach a copy of the email to TAMIS.

For email recipients who do not have zip software, you can create a "self-extracting" file. Please access SEE: Self-Extracting Files for instructions on how to create a self-extracting file.

As an alternative to SecureZip, a TAS employee may follow these steps to encrypt an attachment that is a Microsoft Office 2016, 365, Word or Excel file:

1. Open Word or Excel document;
2. Cloick on the **F**ile tab;
3. Click on **P**rotect **D**ocument;
4. Select **E**ncrypt with **P**assword from the drop-down menu;

5. Create a strong password meeting the software's protocols;
6. Reenter the password and select **O**k; and
7. Inform the taxpayer or representative of this password via telephone. 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. See IRM 13.1.6.7(8). As a last resort, if the employee is unable to contact the taxpayer via phone or leave a voicemail, send the password in a separate email. **Do not transmit the password in the same email as the documents.**

As an alternative to SecureZip, a TAS employee may follow these steps to encrypt an attachment that is in Adobe PDF document:

1. Open the PDF Document;
2. Click on the **T**ools tab;
3. Click on the **P**rotect icon;
4. Select **E**ncrypt;
5. Select **E**ncrypt with **P**assword from the drop-down menu;
6. Under **O**ptions, set compatibility using the drop-down menu to **A**crobat X and later;
7. Verify that **E**ncrypt all document contents is selected;
8. Create a strong password meeting the software's protocols;
9. Select **R**equire a **P**assword to open the document and click **O**k;
10. Enter the password that was created earlier in the pop-up box and click **O**k;
11. Click **F**ile and **S**ave the document; and
12. Inform the taxpayer or representative of this password via telephone. 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. As a last resort, if the employee is unable to contact the taxpayer via phone or leave a voicemail, send the password in a separate email. **Do not transmit the password in the same email as the documents.**

NOTE: Digitally signed PDF documents cannot be encrypted.

For additional information, the U.S. Department of Treasury website contains a

link on "How to encrypt/password protect Microsoft Office and Adobe Acrobat (PDF) documents."

Important Reminder: Employees must use the instructions above to send an encrypted email attachment to taxpayers or representatives. 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 representative. Doing so increases the risk of the email being blocked by the *Safeguarding Personally Identifiable Information Data Extracts (SPIIDE) Automated Data Loss Prevention (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 AC 9600761.

Receiving Documents Electronically from Taxpayers

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 (including Congressional Offices) has already been authenticated pursuant to IRM 13.1.16.2.1, *Disclosure*. In addition, verbally verify the email address.
2. Advise the taxpayer or representative 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 via SecureZip as much as possible. The document must be in one of the file types specified below.

3. As discussed below, if the document contains a signature, the taxpayer or representative 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 representative and document the attempts in the TAMIS history. ***Retransmitting attachments is not required***.
4. 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 representative 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 representative. When in doubt, contact the taxpayer or representative 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 are allowed to 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 (BOD) or function as an attachment to an Operations Assistance Request (OAR), including the following:
    - extensions of statute of limitations on assessment or collection, waivers of statutory notices of deficiency and consents to assessment,
    - agreements to specific tax matters or tax liabilities (closing agreements), and
    - any other statement or form needing the signature of a taxpayer or representative traditionally collected by IRS personnel *outside of standard filing procedures*;
- 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 13.1.8.7, *Disclosure Issues*.

TAS will accept images of signatures (scanned or photographed) in one of the following file types: tiff, jpg, jpeg, pdf, Microsoft Office suite, or Zip. TAS will also accept Digital Signatures that use encryption techniques to provide proof of original and unmodified documentation on one of the following file types: tiff, jpg, jpeg, pdf, Microsoft Office suite, or Zip.

Use of eFax

EFax is still the preferred method of receiving documents from taxpayers or representatives that 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 representative. Instead employees will use their individually assigned email address when choosing to send an email to a taxpayer or representative using the procedures discussed above.

TAS employees may use this temporary digital signature and email guidance until December 31, 2020. 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 representatives. A communication will be issued to inform employees of any extensions of this policy.

Effect on Other Documents:

This IGM supersedes IGM TAS-0420-0009 issued April 13, 2020. 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*.

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

cc: www.irs.gov