Department of the Treasury	Internal Revenue Service	Office of Chief Counsel	**Notice**

CC-2020-002

October 18, 2019

Subject:	Communication with Taxpayers or Representatives by Email	**Cancel Date**:	Upon incorporation into CCDM

Purpose

This Notice announces procedures for Chief Counsel employees to transmit email containing return information or personally identifiable information (PII) to taxpayers or their representatives in Tax Court litigation and in conjunction with requests for letter rulings or closing agreements.

Background

The IRM currently authorizes Chief Counsel to send taxpayers brief scheduling email messages not containing sensitive information, IRM 10.5.1.6.8.1(2), but generally prohibits the sending of PII or return information to external parties without use of approved encryption methods. *See* IRM 10.5.1.6.2.1. The IRM does permit use of encrypted email to send PII and return information to certain authorized external stakeholders such as government agencies, expert witnesses, or cleared contractors. IRM 10.5.1.6.8.2. However, the IRM has to date restricted the use of email to taxpayers or their representatives to exchange PII and return information, including in Tax Court litigation and in conjunction with requests for letter rulings or closing agreements. *See* IRM 10.5.1.6.8.1(1).

Effectively immediately, Chief Counsel employees may exchange PII and return information with taxpayers or their representatives during Tax Court litigation and letter ruling or closing agreement processes, using one of two email encryption methods:

1. The **LB&I Secure Email System** (SEMS), which authorizes the exchange of encryption certificates under specific circumstances, allowing the exchange of fully-encrypted emails and attachments, and

2. **SecureZIP** encrypted email attachments, allowing the sending of password-protected encrypted email attachments to anyone with a compatible zip utility.

Counsel should use SEMS with taxpayer representatives that have the technical sophistication needed to use it. For taxpayers and for taxpayer representatives that cannot use SEMS, Counsel may use SecureZIP to send password-encrypted attachments. Before Counsel may use either email encryption method, the taxpayer must execute and return a Memorandum of Understanding (MOU) agreeing to the use of an email encryption method and acknowledging the risks of using email to send PII and return information.

Distribute to:	Tax Litigation staff	Tax Litigation staff & Support personnel	
	X All Personnel	Electronic Reading Room	
Filename:	CC-2020-002	File copy in:	CC:FM:PFD

Encrypted email to other authorized external stakeholders such as government agencies (including DOJ), expert witnesses, and cleared contractors may continue to be sent using either encryption method without an MOU.

Procedures

Before using either SEMS or SecureZIP to send email containing encrypted PII or return information to taxpayers or their representatives, Counsel employees must first discuss the use of encrypted email with the taxpayer or representative and confirm the identity of the email recipient. This can be done in a face-to-face meeting or by telephone. To further ensure that Counsel is dealing with the taxpayer or authorized representative, all initial email communications with the taxpayer or representative used in establishing the MOU and in establishing the associated list of email addresses authorized to receive encrypted content should be made only to the specific email address or telephone number (i) included in Petitioner's Tax Court pleading signature block pursuant to T.C. Rule 23(a)(3), or (ii) in the original request for a letter ruling, closing agreement, or accompanying Form 2848, Power of Attorney and Declaration of Representative. *See* CCDM 32.3.2.3; IRB 2019-1 §7.01(15).

Regardless of the encryption method used, before sending documents to taxpayers or their representatives, editing history and other metadata must be removed using the "inspect document" function in Microsoft Office or by converting electronic documents to Adobe PDF format.

Use of SEMS

LB&I's authorized SEMS program is intended for use by authorized taxpayer representatives (but not individual taxpayers) that have the technical ability to exchange email encrypted with Secure/Multipurpose Internet Mail Extensions (S/MIME) certificates. SEMS encrypts both attachments and the body of emails and is the type of encryption used with internal IRS email. External parties must exchange S/MIME certificates with the Counsel employees with whom they will be emailing. This requires the external party to use a compatible email system such as Microsoft Outlook, and to have the technical sophistication to exchange and install S/MIME certificates.

To use SEMS, follow the directions available at <this link>. Because SEMS will not encrypt the subject line of the email, do not include PII or return information in the subject line.

Before Counsel employees may use SEMS to send email containing PII or return information to taxpayer representatives, the taxpayer (not merely the representative) must execute a MOU acknowledging the risks inherent in use of email and authorizing the exchange of encrypted email with their representative.

The required MOU language for SEMS is contained in Attachment A.

The taxpayer must return the executed memorandum to Counsel before any encrypted email containing PII or return information may be sent, and the MOU must be retained in the case file.

Use of SecureZIP

SecureZIP is a compression utility that allows the password-enabled encryption of email attachments and other files. To use SecureZIP, both the sender and recipient must have

SecureZIP or a compatible decompression/decryption utility installed (several compatible free utilities exist, including PKWARE's ZIP Reader). Counsel employees may use SecureZIP to email encrypted attachments to authorized external stakeholders, including taxpayers and taxpayer representatives unable to use the LBI Secure Email Program. As noted above, if a taxpayer representative is able to use the LBI Secure Email Program, that method of encryption should be used instead of SecureZIP.

To use SecureZIP to compress and encrypt email attachments, follow the directions available at <this link>. Because SecureZIP will not encrypt either the subject line or the body of the email, all PII, return information, and other information about specific tax matters must be included only in the encrypted attachment.

With SecureZIP enabled, after clicking "send," a dialogue box opens asking if the user would like to zip the message. Select the "encrypt attachments" and "include unzip instructions" checkboxes and click "next." The next dialogue box will ask the user to type and confirm an 8-character minimum password. Record the password for future reference.

The password should never be sent in the same email with the encrypted attachment. It should be provided to the recipient by telephone or in a separate email. Never put the password in the body of the email with the encrypted attachment.

Before Counsel employees may email encrypted email with encrypted attachments containing PII or return information to taxpayers or taxpayer representatives, the taxpayer must execute a MOU acknowledging the risks inherent in use of email and authorizing the exchange of encrypted email attachments.

The MOU for SecureZIP is contained in Attachment B.

The taxpayer must return the executed memorandum to Chief Counsel before any encrypted email attachments containing PII or return information may be sent, and the MOU must be retained in the case file.

Technical questions about how to use encrypted email or encrypted email attachments to securely send return information or PII should be directed to the Counsel BSP hotline at 202-317-4469. Questions about this notice should be directed to the Office of the Associate Chief Counsel (Procedure and Administration) at 202-317-3400.

/s/
Kathryn A. Zuba
Associate Chief Counsel
(Procedure & Administration)

Attachment A
Memorandum of Understanding
Agreement to Use Secure Email System

Generally, the Office of Chief Counsel, Internal Revenue Service (Chief Counsel) communicates with taxpayers or their representatives by sending documents through the mail, or by telephone. In many cases, communication by email is more convenient for both the taxpayer and Chief Counsel. There are risks associated with email, such as the possibility sensitive taxpayer information could be intercepted. If an email is intercepted, any personal information in the email could be viewed by unauthorized persons. It is important to secure email using appropriate encryption, particularly when transmitting sensitive or confidential tax-related information. This agreement is intended to enhance the process of securely exchanging taxpayer data and other tax-related information and increase efficiency of interaction between Chief Counsel and taxpayers or their representatives.

1. Communications

In order to communicate in a formal, efficient manner for tax issues, written communication is essential. Email is one form of written communication; however, in order to protect sensitive information, additional safeguards are necessary for email communications which are not generally required for paper documents. Chief Counsel and the taxpayer, by this agreement, consent to written communications being transmitted via secure email. In order to limit access to this information, Chief Counsel and the taxpayer agree to designate participants and provide the list of participants in an addendum to this agreement. Only individuals designated as participants by Chief Counsel and the taxpayer on that list will be included in these communications. The taxpayer will be responsible for providing an updated list when there are changes to their designated participants.

2. The Secure Email System (SEMS)

Secure email involves sending emails through a data encryption process which complies with S/MIME (Secure / Multipurpose Internet Mail Extensions) standards, a protocol that adds digital signatures and encryption to email. To accomplish this, an initial exchange of digitally signed email messages will be required.

3. Security

Both parties agree to work together to ensure the joint security of the information contained in the encrypted email. Pursuant to this MOU, Chief Counsel certifies that its system used to transmit, store, or process data is designed, managed, and operated in a secure manner in compliance with relevant laws, regulations, and policies. The taxpayer should also undertake steps to ensure proper security protections are employed to transmit, receive, and store this information. By signing this agreement, the taxpayer understands that only encrypted email should be used by the taxpayer in communicating with the IRS.

Even with encryption it is possible electronic communications could be intercepted. By signing this agreement, the taxpayer acknowledges that the United States Government does not guarantee the security of data transmitted electronically by email and accepts no liability, regardless of fault, for any loss or damage sustained without negligence of United States Government employees.

4. Costs

Both parties agree to bear all of their own costs on a nonreimbursable basis in complying with this agreement.

5. Timeline

This agreement is effective upon the signatures of both parties and will remain in effect for the duration of the matter in Chief Counsel, including, but not limited to such time as the matter is on appeal or pending before other United States Government agencies such as the Department of the Treasury or Department of Justice. As a new participant is added to the MOU, they are added to the addendum and both the MOU and the addendum remain part of the case or administrative file. If either the taxpayer or Chief Counsel wishes to terminate this agreement before it expires, it may be done upon thirty (30) days' advance notice.

In the event of a security incident, Chief Counsel may immediately terminate the agreement.

6 Additional Terms

Nothing in this agreement shall be construed as a waiver of any sovereign immunity of the United States Government. This agreement is not intended to contravene in any way, the precedence or applicability of Federal law and shall be governed by and construed under Federal law of the United States of America.

(Name of Taxpayer)
(Title of Individual Signing Agreement)

SIGNATURE: _____

DATE: _____

Office of Chief Counsel, Internal Revenue Service, United States of America
(Name of Counsel Employee)
(Title of Counsel Employee Signing Agreement)

SIGNATURE: _____

DATE: _____

Addendum: Individuals and Email Addresses Authorized
Pursuant to This Memorandum of Understanding

Authorized Person Name	Authorized Email Address	Phone Number

Attachment B
Memorandum of Understanding
Agreement to Use Encrypted Email Attachments

Generally, the Office of Chief Counsel, Internal Revenue Service (Chief Counsel) communicates with taxpayers or their representatives by sending documents through the mail or via facsimile, or by telephone. In many cases communication by email is more convenient for both the taxpayer and Chief Counsel. There are risks associated with email, such as the possibility sensitive taxpayer information could be intercepted. If an email is intercepted, any personal information in the email could be viewed by unauthorized persons. It is important to secure email using appropriate encryption, particularly when transmitting sensitive or confidential tax-related information. This agreement is intended to enhance the process of securely exchanging taxpayer data and other tax-related information and increase efficiency of interaction between Chief Counsel and taxpayers or their representatives.

1. Communications

In order to communicate in a formal, efficient manner for tax issues, written communication is essential. Email is one form of written communication; however, in order to protect sensitive information, additional safeguards are necessary for email communications which are not generally required for paper documents. Chief Counsel and the taxpayer, by this agreement, consent to written communications being transmitted via encrypted email attachments. In order to limit access to this information, Chief Counsel and the taxpayer agree to designate participants and provide the list of participants in an addendum to this agreement. Only individuals designated as participants by Chief Counsel and the taxpayer on that list will be included in these communications. The taxpayer will be responsible for providing an updated list when there are changes to their designated participants.

2. Encrypted Email Attachments

Chief Counsel uses SecureZIP®, a commercial program, to compress and encrypt email attachments that contain sensitive information. The recipient of encrypted email attachments created using this utility may decrypt and view them by entering a password. The recipient must first install a compatible "zip" software utility. In addition to SecureZIP®, compatible utilities include PKZIP®, and ZIP Reader® by PKWARE®, which is a free Windows utility that enables users to process compressed and/or AES passphrase-encrypted files created by SecureZIP®, PKZIP® and other products that support these capabilities.
SecureZIP and compatible utilities only encrypt the email attachment and not the subject line nor the body of the email itself. To prevent interception and viewing of sensitive or other confidential tax-related information by unauthorized persons, such information must not be included in the email body or subject line.

3. Security

Both parties agree to work together to ensure the joint security of the information contained in the encrypted email attachment. Pursuant to this MOU, Chief Counsel certifies that its system used to transmit, store, or process data is designed, managed, and operated in a secure manner in compliance with relevant laws, regulations, and policies. The taxpayer should also undertake steps to ensure proper security protections are employed to transmit, receive, and store this information. By signing this agreement, the taxpayer understands that sensitive or confidential information should be sent only by encrypted email attachment in communicating with the IRS.

Even with encryption it is possible electronic communications could be intercepted. By signing this agreement, the taxpayer acknowledges that the United States Government does not

guarantee the security of data transmitted electronically by email and accepts no liability, regardless of fault, for any loss or damage sustained without negligence of United States Government employees.

4. Costs

Both parties agree to bear all of their own costs on a nonreimbursable basis in complying with this agreement.

5. Timeline

This agreement is effective upon the signatures of both parties and will remain in effect for the duration of the matter in Chief Counsel, including, but not limited to such time as the matter is on appeal or pending before other United States Government agencies such as the Department of the Treasury or Department of Justice. As a new participant is added to the MOU, they are added to the addendum and both the MOU and the addendum remain part of the case or administrative file. If either the taxpayer or Chief Counsel wishes to terminate this agreement before it expires, it may be done upon thirty (30) days' advance notice.

In the event of a security incident, Chief Counsel may immediately terminate the agreement.

6 Additional Terms

Nothing in this agreement shall be construed as a waiver of any sovereign immunity of the United States Government. This agreement is not intended to contravene in any way, the precedence or applicability of Federal law and shall be governed by and construed under Federal law of the United States of America.

(Name of Taxpayer)
(Title of Individual Signing Agreement)

SIGNATURE: _____

DATE: _____

Office of Chief Counsel, Internal Revenue Service, United States of America
(Name of Counsel Employee)
(Title of Counsel Employee Signing Agreement)

SIGNATURE: _____

DATE: _____

Addendum: Individuals and Email Addresses Authorized
Pursuant to This Memorandum of Understanding

Authorized Person Name	Authorized Email Address	Phone Number