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

CC-2020-007

June 15, 2020

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

Purpose

This Notice adds two additional encryption options 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, in addition to the options set out in Chief Counsel Notice CC-2020-002.

Discussion

Chief Counsel Notice CC-2020-002 set out a procedure for Chief Counsel employees to send email containing return information or PII to taxpayers or their representatives, using either the SEMS email encryption system or SecureZIP to encrypt email attachments. Chief Counsel employees may now also use Adobe Acrobat Pro password encryption to encrypt and send email attachments in Adobe Portable Document Format (.pdf), and Microsoft Office 365 Protect Document to encrypt and send email attachments in Microsoft Office formats.

Documents encrypted with Adobe Acrobat Pro password encryption or Microsoft Office 365 Protect Document password encryption may be easier for many recipients to open, particularly recipients who have difficulties using SEMS or SecureZIP (the encryption methods originally described in Chief Counsel Notice 2020-002). Documents encrypted with Adobe Acrobat Pro may be opened and decrypted with recent versions of Adobe Acrobat, or with the free Acrobat Reader DC which is widely distributed and available for free download. Documents encrypted with Office 365 may be opened and decrypted with Microsoft Office 2016 or Microsoft Office 365.

How to Encrypt Using Adobe Acrobat Pro

The files to be encrypted must be in or converted to Adobe .pdf format before they can be encrypted and attached to an email. For electronic files, this can be done within Microsoft Office or the Adobe Acrobat Pro software installed on Chief Counsel computers. Paper files may be scanned to .pdf format using an IRS scanner or multifunction copier/scanner.

The Chief Counsel sender's Adobe Acrobat Pro software must first be properly configured to support 256-bit AES password encryption. Adobe .pdf attachments containing PII or return information must be sent to external recipients using this encryption level. Detailed instructions for doing so are appended to this Notice in **Attachment A**.

Distribute to:	Tax Litigation staff	Tax Litigation staff & Support personnel
	X All Personnel	Electronic Reading Room
Filename:	CC-2020-007	File copy in: CC:FM:PFD

How to Encrypt Using Office 365

Either Office 365 Office 2016 may also be used to encrypt Microsoft Office files. Note that the encryption levels in earlier versions of Office do not meet IRS security standards, so they should not be used. The files to be encrypted must be in an Office format, such as Word, Excel, or PowerPoint. Detailed instructions for encrypting Office 365 files are appended to this Notice in **Attachment A**.

Memorandum of Understanding

Before sending encrypted attachments to a taxpayer or representative, the taxpayer must execute and return a Memorandum of Understanding (MOU) agreeing to the use of the specified email encryption method and acknowledging the risks of using email to send PII and return information, as set forth in CCDM 30.6.1.2.3(4) and Chief Counsel Notice 2020-002. An MOU for Adobe .pdf encryption is attached to this Notice as **Attachment B** and is also available as a Microsoft Word document on the Litigation Technology page of the Chief Counsel Intranet. An MOU for Microsoft Office 365 encryption is attached to this Notice as **Attachment C**, and is also available as a Microsoft Word document on the Litigation Technology page of the Chief Counsel Intranet.

The taxpayer must return the executed MOU 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 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 202-317-5388.

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

Attachment A

How to Encrypt a Document using Adobe Acrobat Pro or Microsoft Office 365

You may encrypt a document for emailing as an attachment using either Adobe Acrobat Pro or Microsoft Office 365 and a password. The recipient will be able to decrypt and open the file with newer versions of Adobe Reader or Acrobat, or with Microsoft Office 2016 or 365. Older versions of either type of software may not successfully decrypt because they support only weaker encryption strengths.

1. Adobe Acrobat Pro Encryption

The files to be encrypted must be in or converted to Adobe .pdf format before encryption and attachment to an email. For electronic files, this can be done within Microsoft Office or the Adobe Acrobat Pro software installed on Chief Counsel computers. Paper files may be scanned to .pdf format using an IRS scanner or multifunction copier/scanner.

Summary of Encryption Method:

- Use the "Encrypt with password" option instead of "Encrypt with certificate"
- Use the Compatibility option "Acrobat X and later" which uses 256-bit AES encryption.
- Use a "strong" password containing lower- and upper-case letters, numbers and special characters.

Detailed Instructions - Encrypting a Document:

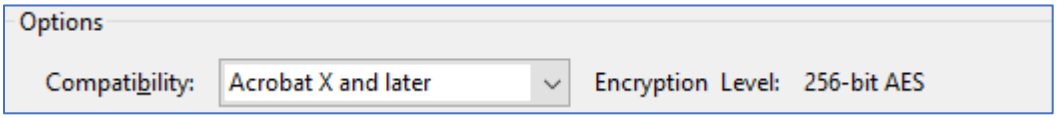
1. Open **Acrobat Pro**
2. Open a file
3. Click **Tools**
4. Click **Protect** on right side or scroll down and click **Protect** under *Protect and Standardize*

   The Protect toolbar displays at the top.

5. Click drop-down arrow on **Encrypt**
6. Click **2 Encrypt with password**
7. Click **Yes** to Applying New Security Setting message, "Are you sure you want to change the security on this document?"

   The **Password Security Settings** screen displays.

8. Under Options towards the bottom of the screen, change the Compatibility to **Adobe X and later**



   Note: If you type the password before changing the Compatibility option, the password may be blanked out and you will need to enter it again.

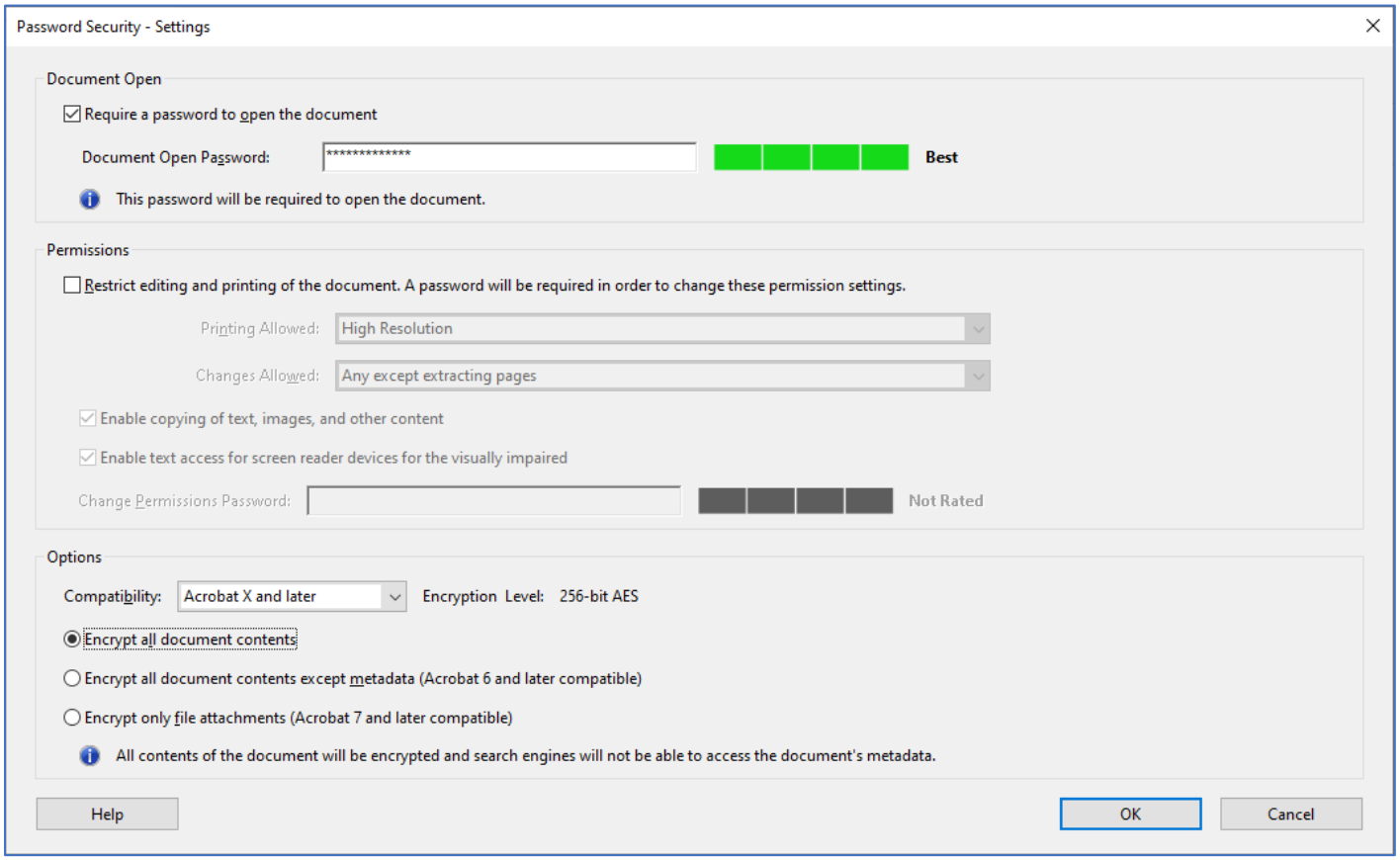
9. Click the checkbox for "Require a password to open this document." at the top of the screen

10. Type in the password in the **Document Open Password** field

    The password entered will be rated on its strength; use upper/lowercase letters, special characters and numbers.

11. Note the password, you will need to pass on to the taxpayer as well as enter it again.

    Following is a sample screenshot with the password and Compatibility option selected:



12. Click **OK**
13. Enter the password again in the Confirm Document Open Password dialogue
14. Click **OK**
15. You may get a warning 'Security settings will not be applied to the document until you save the document. You will be able to continue to change the security settings until you close the document.'
16. Save the document
17. Once you save the document (SECURE) will display after the document name.
18. Close the document
19. Open the document to test the password

2. Microsoft Office 365 Encryption

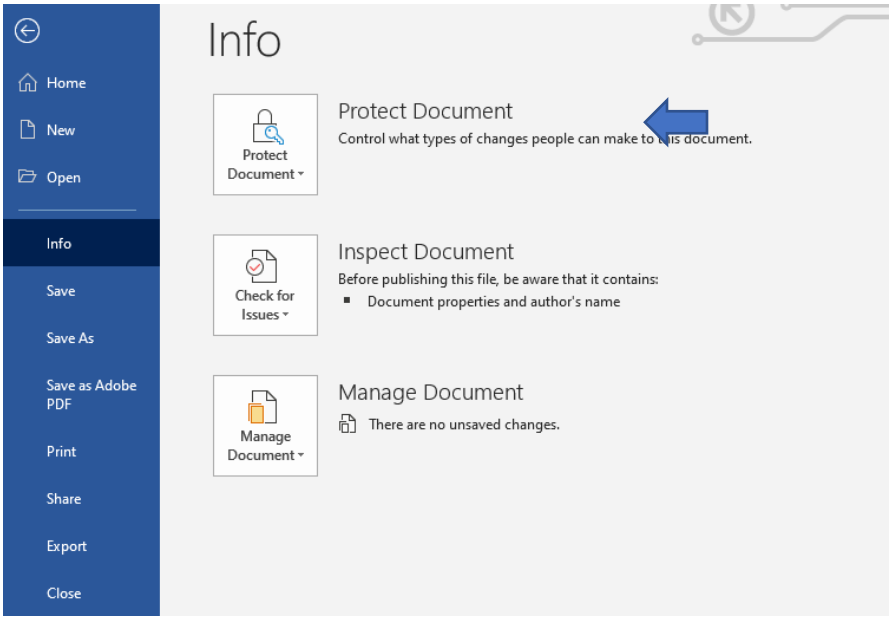
The files to be encrypted must be in a Microsoft Office format before encryption and attachment to an email. Only Chief Counsel users with Microsoft Office 365 installed on their computers may use this encryption method. Encryption in older versions of Microsoft Office is not 256-bit AES encryption, and therefore does not meet IRS standards.

Summary of Encryption Method:

- Use the “Protect Document/Encrypt with password” option on the “File” menu page of the Microsoft application.
- Use a “strong” password containing lower- and upper-case letters, numbers and special characters.

Detailed Instructions - Encrypting a Document (this example uses Microsoft Word; the process is similar in other Office applications):

1. Open **Microsoft Word 365**
2. Open a file
3. Click the **File** menu at the top left of the screen. You will be taken to the file menu page
4. Click the **Protect Document** button from on the File menu page

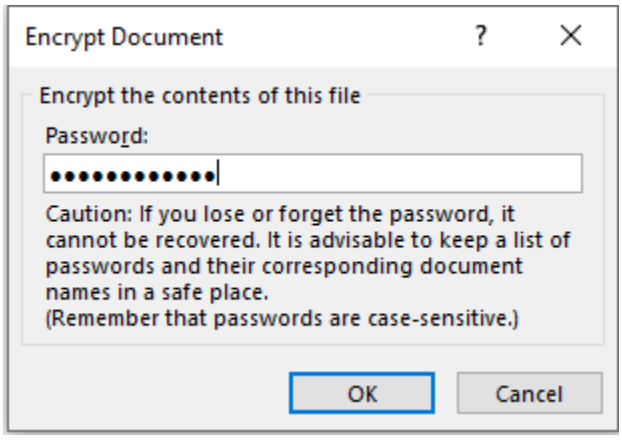


5. Choose **Encrypt with Password** on the drop-down menu that appears

The “Encrypt Document” dialog box appears

6. Type in the password in the **Encrypt Document** dialog box

   The password entered should have upper/lowercase letters, special characters and numbers.



7. Note the password, you will need to pass on to the taxpayer as well as enter it again.

8. Click OK
9. Enter the password again in the **Confirm Password** dialog box
10. Click OK

The **Protect Document** button and block will now be highlighted with a notice that “a password is required to open this document”

11. Save the document
12. Close the document
13. Open the document to test the password

Attachment B

Memorandum of Understanding
Agreement to Use Encrypted Email Attachments
(Adobe .pdf format)

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 Adobe Acrobat Pro®, a commercial program, to compress and encrypt email attachments in Adobe Portable Document Format (.pdf) 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 .pdf software reader with password decryption capability. In addition to Adobe Acrobat Pro®, the Adobe Acrobat DC Reader® is a free Windows utility that enables users to decrypt and open AES passphrase-encrypted files created by Adobe Acrobat Pro. Other compatible .pdf decryption utilities may exist.

Acrobat Pro® only encrypts 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.

Further information about how to encrypt email attachments with Adobe Acrobat products may be found on Adobe's web site or at this link: https://home.treasury.gov/how-to-encryptpassword-protect-microsoft-office-and-adobe-acrobat-pdf-documents

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

Attachment C

Memorandum of Understanding
Agreement to Use Encrypted Email Attachments
(Microsoft Office 2016/365 Password Encryption)

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 Microsoft Office 365®, a commercial program, to compress and encrypt email attachments in Microsoft Office formats, including Word, Excel or PowerPoint, that contain sensitive information. The recipient of encrypted email attachments created using this program may decrypt and view them by entering a password. The recipient should use Microsoft 2016® or Microsoft Office 365® to decrypt and open encrypted Office files sent by Chief Counsel as email attachments. Older versions of Microsoft Office may not successfully decrypt these attachments.

Microsoft Office 365 only encrypts 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.

Further information about how to encrypt email attachments with Microsoft Office products may be found on Microsoft's web site or at this link: https://home.treasury.gov/how-to-encryptpassword-protect-microsoft-office-and-adobe-acrobat-pdf-documents

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