SECURELY TRANSMITTING SENSITIVE INFORMATION

Encrypting Sensitive Information: The Requirements

AFI 10-701: Protect all electronic communications containing critical information and indicators
AFI 33-332: When handling sensitive personally identifiable information (PII) between DoD or other agencies, ensure e-mails are digitally signed, encrypted, or attachments are password protected

Encrypting Sensitive Information: Glossary of Commonly Used Terms

Critical Information – Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively against friendly mission accomplishments.
Digitally Encrypt – The process of converting electronic data into another form, called ciphertext, which cannot be easily understood by anyone except authorized parties.
Digital Certificate – An electronic "passport" that allows a person, computer or organization to exchange information securely over the internet using the public key infrastructure.
Digitally Sign – The process of electronically signing an e-mail, piece of software or document to validate the authenticity /integrity of the message. This does not protect information from unauthorized access.
Personally Identifiable Information – Information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked/linkable to a specific person
Password Protect – A unique password on a document to protect contents from unauthorized access.
Controlled Unclassified Information – Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.

Microsoft Outlook Encryption

After drafting your e-mail, click the **Option** tab then the **Encrypt** button. You may be required to enter your PIN. If an encryption error occurs you may need to retrieve the recipient's certificates as explained in the Adding PKI Certificate sections.
NOTE: You may have the encrypt button on your main toolbar, if so, just click that button.
NOTE: Digitally signing an e-mail only verifies the sender is who they say they are and does NOT protect the information from being read by unauthorized individuals.

Outlook Web Access (OWA) Encryption

Going TDY and need secure access to your e-mail? The Outlook S/MIME controller can be configured to allow you to send/receive encrypted e-mails. Talk to your network professionals for help before you go.

Retrieving Digital Encryption Keys after new CAC

Encrypted e-mail can only be opened with your private encryption key. When the CAC is replaced, previously encrypted e-mails are no longer accessible because you have a new private key. Therefore, you must recover the previous private key in order to open the previously encrypted e-mail. The Air Force Public Key Infrastructure (PKI) System Program Office manages old PKI certificates. You can recover the keys by visiting https://ara-6.csd.disa.mil/ara/search or navigating through vESD on your desktop.

Air Force OPSEC Support Team (AF OST)
Joint Base San Antonio – Lackland AFB
DSN 312-945-3952/2667
Commercial 210-925-3952/2667
AF.OST@us.af.mil
www.facebook.com/AirForceOST/

Dated November 2019

PKI Certificates: Role-Based/Group (i.e., Organizational E-mail Accounts)

Role based certificates and group certificates can be issued to an individual filling a specific role or for use in an organizational e-mail account to support e-mail encryption. Specific implementation procedures are outlined in AFMAN 17-1301. This process is managed by the Local Registration Authority on your installation. For additional information please visit https://cyber.mil/pki-pke/.

Adding PKI Certificates: DoD White Pages

The DoD White Pages allows you to retrieve someone else's public key certificate and add it to your Outlook address book.

- Navigate to https://www.whitepages.mil/ or https://dod411.gds.disa.mil/
- Enter search terms
- Choose certificate you would like to utilize
- Follow prompts to download into Outlook address book

Alternative if Encryption is Unavailable: Password Protecting Attachments

Microsoft Office documents can be password protected before being sent as an attachment offering some protection to the document. The steps are the same for all Office documents:

- Click the **File** tab on the main tool bar
- You will see three large buttons appear
- Click the **Protect Presentation** (Workbook, Document, etc.) button
- Scroll and click the **Encrypt with Password** button
- Enter a password and press **OK**
- Re-enter the password and press **OK**

NOTE: The encryption password should never be included in the same e-mail with the attachment. This option should only be used if all other attempts to encrypt the information have been exhausted.

Alternative Encryption Tools: DOTS

The DoDIIS One-way Transfer Service (DOTS) tool allows you to upload information from an unclassified network to classified networks for further dissemination

- Navigate to https://dots.dodiis.mil/
- Enter a recipient e-mail address (Note: the e-mail must be for the secure network)
- Click the **Add** button
- Navigate to the file you want to upload; click the **Open** button
- Click the **Upload** button
- Click the **Done** button
- The recipient will receive an e-mail on the secure network indicating a file is ready
  NOTE: Available on SIPRNet at https://dots.dia.smil.mil to transfer information to JWICS.

Alternative Encryption Tools: Encryption Wizard

Encryption Wizard is a tool created by the Air Force Research Lab and provided under the Software Protection Initiative. It is available for government and public use. This tool has been approved for use on the NIPRNet and requires a software download.

- Navigate to http://spi.dod.mil/ewizard.htm
- In the menu on the left click on Encryption Wizard
- Choose which edition you need to download and follow the onscreen directions

NOTE: The public version of the tool is great to use to protect your personal files on your home system.

Alternative Encryption Tools: DoD Secure Access File Exchange (SAFE)

DoD SAFE is an application for securely exchanging files when standard encryption is unavailable. This tool is a great alternative to emailing files larger than 1 MB as well as transferring files from a .mil/.gov to a .com/.edu type address

- Navigate to: https://safe.apps.mil/
- For detailed instructions, select Help icon at the top of the screen
- Follow the directions in the guide for the proper use of SAFE

For assistance and tips for using these methods to securely transmit your sensitive information please contact your local OPSEC representative.