

This Overall Classification of this Presentation is
Unclassified



Email Weapon System (EWS)

(AKA: Microsoft Outlook)

LCDR Greg Taylor
BUPERS IAM

The information presented in this brief is current as of 17 January 2012



What Do All of These Have in Common?





Email Weapon System (EWS)

The image shows a screenshot of an email client window titled "Untitled - Message (Plain Text)". The interface includes a menu bar (Message, Insert, Options, Format Text, Adobe PDF) and a ribbon with various toolbars. Annotations in red text with arrows point to specific elements:

- Launch Button:** Points to the "Send" button on the left side of the email composition area.
- Payload:** Points to the large empty text area at the bottom of the window, which is where the message content is entered.
- Targets:** Points to the "To..." and "Cc..." fields in the recipient list.
- Safeties:** Points to a red circle in the "Options" toolbar, which contains icons for "Follow Up", "Spelling", and "Proofing".



Presentation Outline

- Policy & Guidance
- Email Encryption
- Unclassified, Sensitive Information
- Sensitive vs. Non-sensitive PII
- Email Encryption Example
- Digital Signature
- **Ready... Aim... Fire...**
- Misfire Procedures
- Troubleshooting Techniques
- Understanding Common Alerts
- Affects of Digital Signature and Encryption on Email Size
- PII Breach Reporting Procedures
- Myths Debunked
- Moving Forward



Policy & Guidance

- [R 071651Z DEC 04 CNO WASHINGTON DC](#)
 - DIGITALLY SIGNING E-MAIL SENT WITHIN DOD HAS BEEN REQUIRED SINCE 1 APRIL 2004, OR AS THE WORKSTATION HARDWARE IS PROVIDED. E-MAIL REQUIRING MESSAGE INTEGRITY AND/OR NON-REPUDIATION MUST BE DIGITALLY SIGNED.
 - ENCRYPT E-MAIL CONTAINING SENSITIVE INFORMATION AS DEFINED BY REF B (E.G., PRIVACY ACT INFO, HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT INFO, CONTRACT INFO, FOUO, ETC.) AND E-MAIL THAT DISCUSSES ANY MATTER THAT MAY SERVE AS AN OPSEC INDICATOR.
- [NAVADMIN 248/08](#)
 - DIGITAL SIGNING OF EMAILS IS A REQUIREMENT ACROSS DOD. ALL EMAILS REQUIRING DATA INTEGRITY, MESSAGE AUTHENTICITY, AND/OR NONREPUDIATION MUST BE DIGITALLY SIGNED. THIS INCLUDES ANY EMAIL THAT:
 - A. DIRECTS, TASKS, OR PASSES DIRECTION OR TASKING.
 - B. REQUESTS OR RESPONDS TO REQUESTS FOR RESOURCES.
 - C. PROMULGATES ORGANIZATION, POSITION, OR INFORMATION EXTERNAL TO THE ORGANIZATION (DIVISION, DEPARTMENT, OR COMMAND).
 - D. DISCUSSES ANY OPERATIONAL MATTER.
 - E. DISCUSSES CONTRACT INFORMATION, FINANCIAL, OR FUNDING MATTER.
 - F. DISCUSSES PERSONNEL MANAGEMENT MATTERS.
 - G. THE NEED EXISTS TO ENSURE THAT THE EMAIL ORIGINATOR IS THE ACTUAL AUTHOR.
 - H. THE NEED EXISTS TO ENSURE THAT THE EMAIL HAS NOT BEEN TAMPERED WITH IN TRANSIT.
 - I. IS SENT FROM A DOD-OWNED SYSTEM OR ACCOUNT WHICH CONTAIN AN EMBEDDED HYPERLINK (E.G., ACTIVE LINK TO A WEB PAGE, WEB PORTAL, ETC.) MUST BE DIGITALLY SIGNED. PURE TEXT REFERENCES (NON-ACTIVE INTERNET LINKS) TO WEB ADDRESSES, UNIFORM RESOURCE LOCATORS (URL), OR EMAIL ADDRESSES DO NOT REQUIRE A DIGITAL SIGNATURE.
 - J. IS SENT FROM A DOD-OWNED SYSTEM OR ACCOUNT WHICH CONTAIN AN ATTACHMENT (ANY TYPE OF ATTACHED FILE) MUST BE DIGITALLY SIGNED.
- DON CIO Resources:
 - [DON Digital Signature and Encryption Policy for Emails Containing PII](#)
 - How to sign and encrypt emails
 - Marking of emails containing sensitive data or attachments



Email Encryption

- Must be used for emails containing unclassified, sensitive information.
- Used to provide reasonable assurance that the email can only be accessed by the intended recipient(s). (Confidentiality)
- Accomplished using both symmetric (one key used for both encryption and decryption) and asymmetric (key pair is used: one for encryption, one for decryption, and vice versa) methods.
- Protects both the message and the attachment(s).
- Must be selected manually for each individual email. Outlook can be configured for automatic encryption, but this setting cannot be changed permanently. Follow the procedure below to temporarily set encryption as a default:

Outlook: Tools -> Trust Center -> E-mail Security -> Encrypt contents and attachments for outgoing messages



Unclassified, Sensitive Information

- From Navy Policy:
 - Privacy Act info (the [DoD 5400.11-R](#) (p. 39) lists information types that are normally releasable)
 - Health Insurance Portability and Accountability (HIPAA) info
 - Contract info
 - For Official Use Only info (the [DoD 5200.1-R](#) (p. 138) lists the FOUO exemption categories)
 - OPSEC indicators
- Others:
 - Pre-decisional info
 - Other information deemed sensitive by the originator



Sensitive vs. Non-sensitive PII

Must be protected

Sensitive PII includes but is not limited to:

- Name and other names used (in a sensitive context);
- Social Security number, full and truncated;
- Driver's license and other identification numbers;
- Citizenship, legal status, gender, race/ethnicity;
- Birth date, place of birth;
- Home and personal cell telephone numbers;
- Personal email address, mailing and home address;
- Religious preference;
- Security clearance;
- Mother's middle and maiden names;
- Spouse information, marital status, child information, emergency contact information;
- Biometrics;
- Financial information, medical information, disability information;
- Law enforcement information, employment information, educational information; and
- Military records.

PII, but usually does not need to be protected

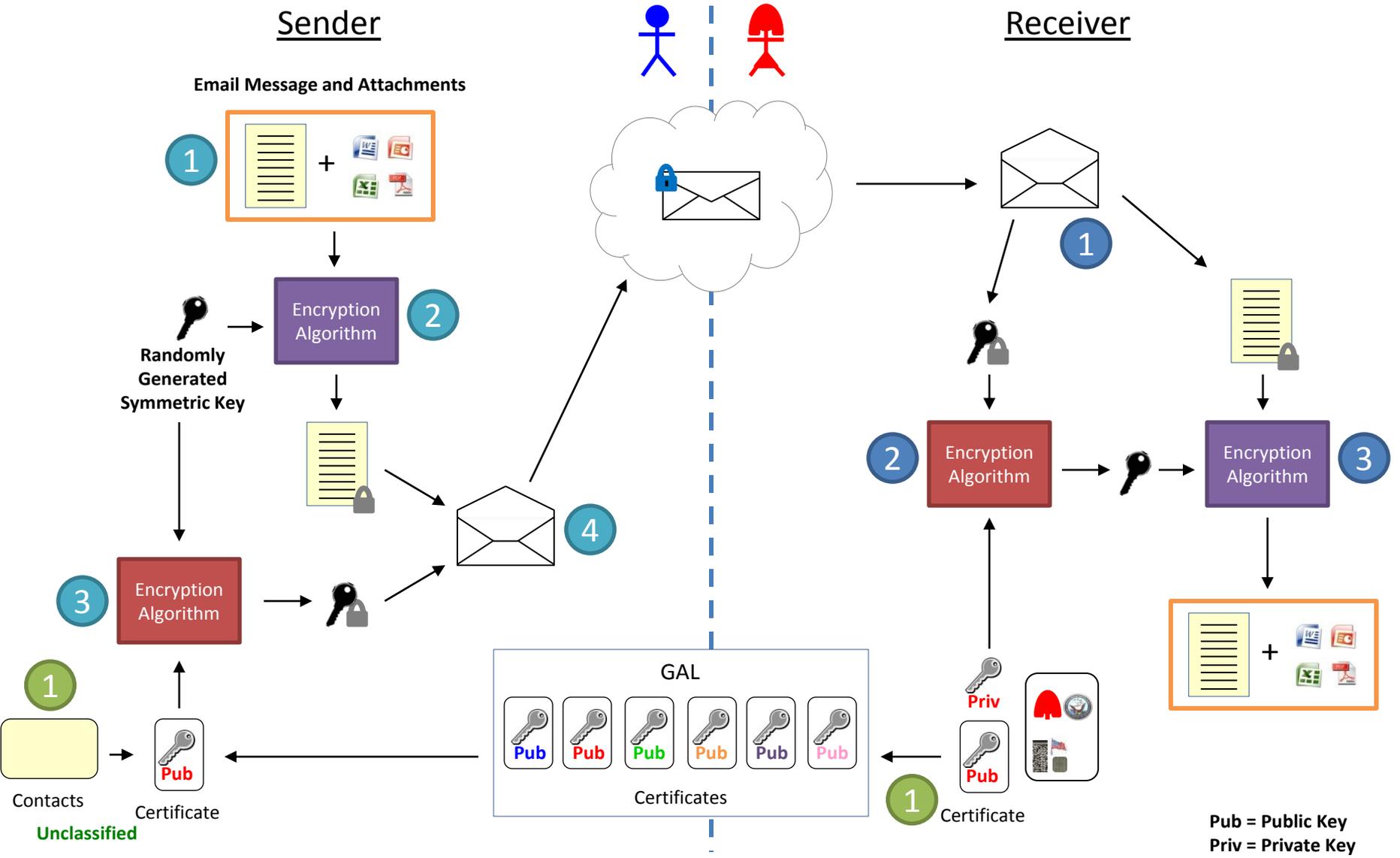
Non-sensitive PII includes but is not limited to:

- Name and other names used (in a non-sensitive context);
- Rank;
- Office location;
- Business telephone number;
- Business email address;
- Badge number; and
- Other information that is releasable to the public.

Note: The context of the information must also be taken into account when determining if it is sensitive or non-sensitive PII. For example, a list of personnel with office phone numbers would be considered non-sensitive PII. However, if this same list also indicated that these individuals had contracted a terminal disease, it would now be considered sensitive PII.



Email Encryption Example



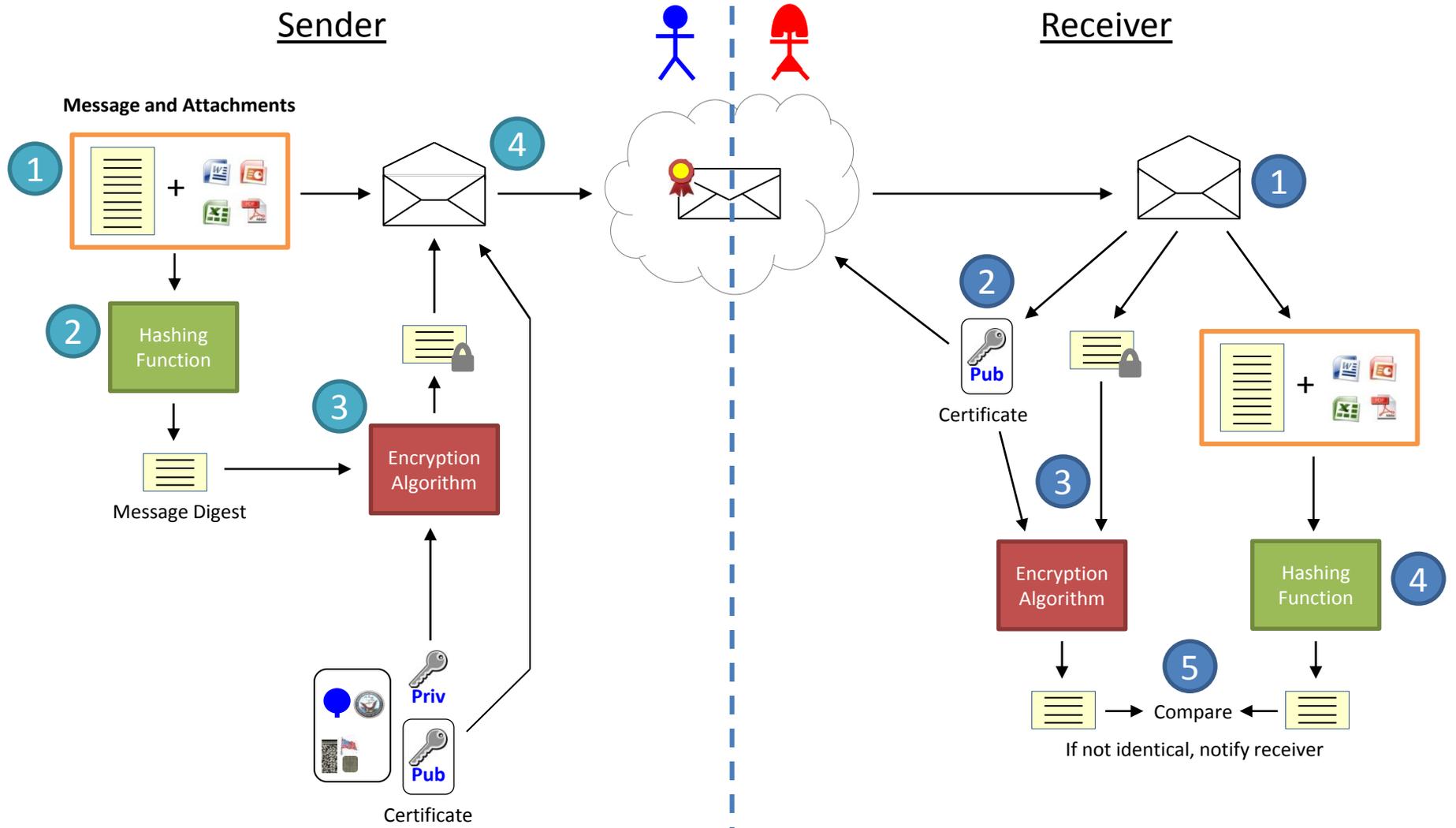


Digital Signature

- Must be used for emails containing official business, attachments, or embedded links.
- Used to provide reasonable assurance that an email message has not been modified in transit (Integrity) and that the sender of the message is who he/she claims to be (Authenticity).
- Inability of sender to deny that he/she sent a message (Non-Repudiation).
- Provides no confidentiality. Message digest is encrypted – not the message. Message and attachments can be sent to and read by any recipient.
- Default setting for Outlook on NMCI machines has digital signature selected.



Email Digital Signature Example





Ready... Aim... Fire!

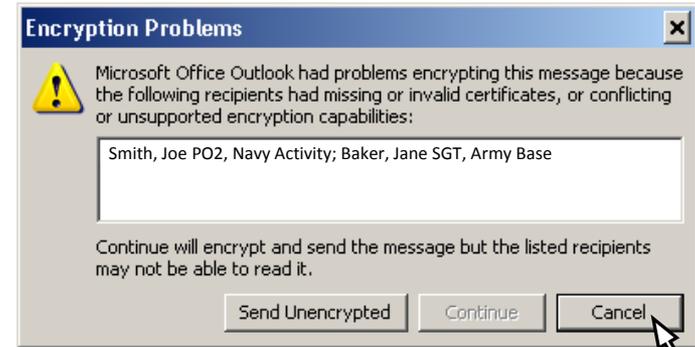
- Ready: Draft, attach, digitally sign (if not already selected), and encrypt (if required).
 - Open each attachment to ensure only intended files are attached.
 - If the email body or attachment contains sensitive PII, add (FOUO) to the subject line
 - If the email body contains sensitive PII, mark the email with “FOR OFFICIAL USE ONLY - PRIVACY ACT SENSITIVE: Any misuse or unauthorized disclosure of this information may result in both criminal and civil penalties.”
 - If an attachment contains sensitive PII, add “Attachment is FOUO” at the top of the message. Attachments containing PII should also have a filename beginning with (FOUO).
- Aim: If the email contains sensitive information, ensure the recipients selected have a need to know. Ensure name(s) selected from the GAL represent the actual intended recipients (e.g., there are 46 John Smiths).
- Fire: Click “Send”

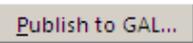
If email failed to send due to encryption issues, follow “misfire” procedures on the next slide.

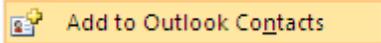


Misfire Procedures

- DO NOT select “Send Unencrypted”
- Select “Cancel” and remove failed recipient addresses from the email
- Click “Send”
- Send separate email to unsupported email addresses requesting a reply with a digitally signed email (address not in the GAL) or to reply after publishing their certificates (address in the GAL).



To publish certificates: Outlook: Tools -> Trust Center -> E-mail Security -> 

- Right-click on name in email reply and select 
- Click  on the contact and attempt to send the encrypted email again.

Note: If using NMCI, published certificates may not be available for a few minutes while servers replicate and/or if the user’s GAL is not synced. To manually sync GAL, follow the procedure below:

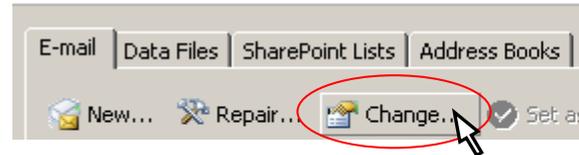
My Computer: System (C:) -> Program Files -> Microsoft Office -> GlobalDirectory ->  GALSyncU.exe



Additional Troubleshooting Techniques (NMCI)

- If a valid certificate is verified for the recipient, and the email still cannot be sent encrypted, try the following:
 - Go to the Outlook toolbar and click on the small arrow next to the  button, then download the address book with “Full Details” (may take 5-10 minutes). Attempt to send encrypted email again.
 - ‘Cached Exchange Mode’ can also cause encryption problems. To check to see if you are in this mode, perform the following in Outlook:

Tools -> Account Settings -> E-mail Security ->



If is checked, uncheck it and then attempt to send encrypted email again (note: you will be required to shutdown and restart Outlook for the new settings to take effect). Recheck after email is sent (if desired).

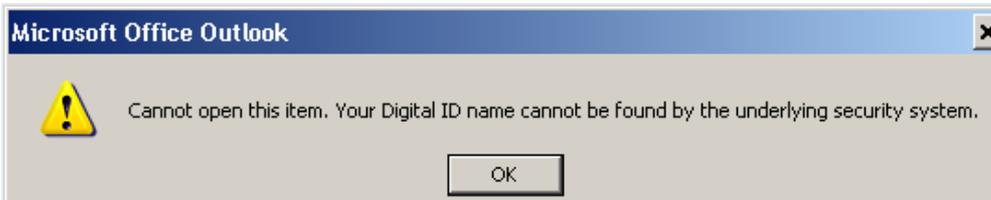


Understanding Common Alerts

- Invalid digital signature



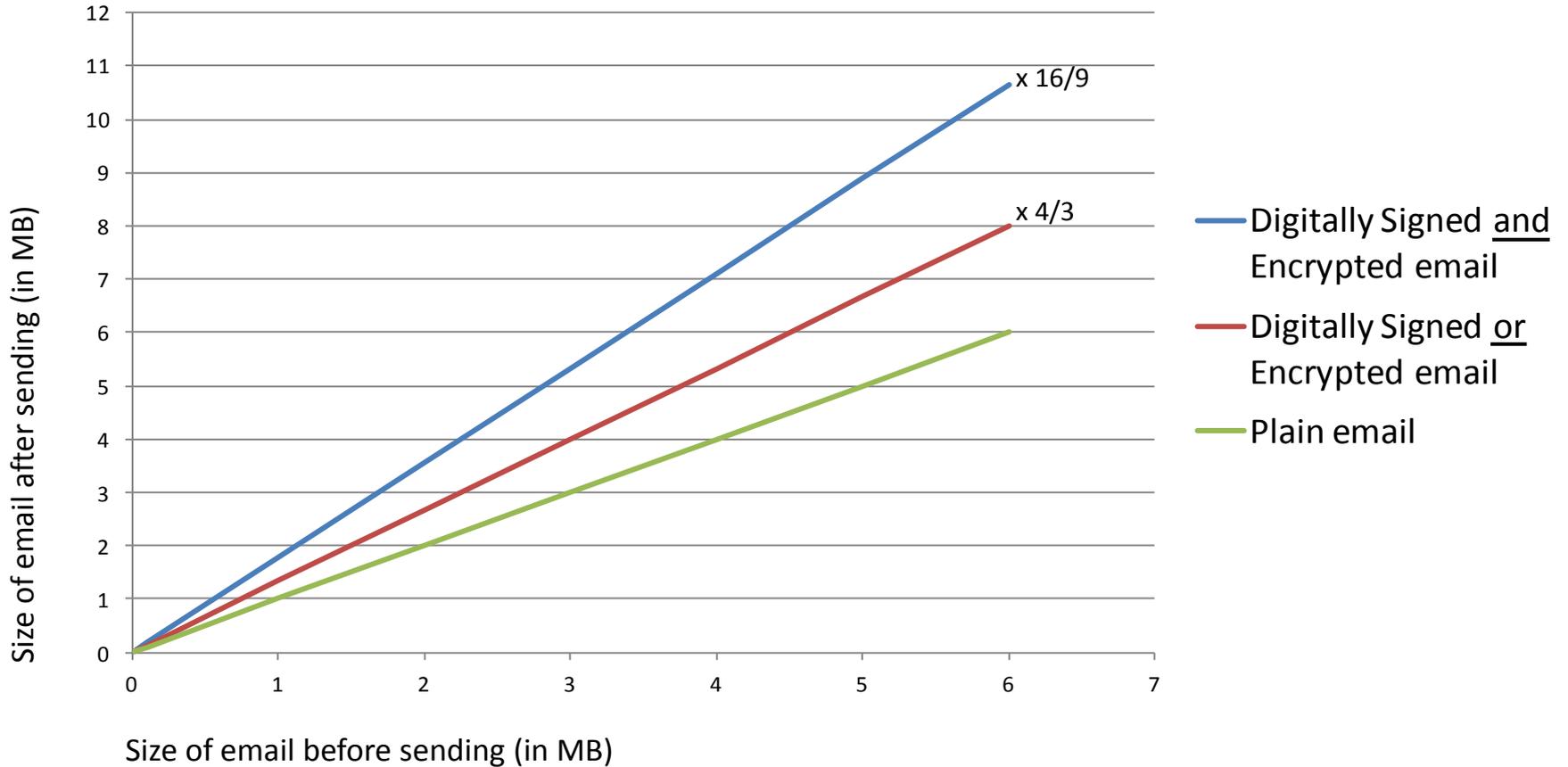
- Inability to open old encrypted emails



- Go to: <https://ara-1.c3pki.chamb.disa.mil/ara/Key>
- Select the appropriate key to recover, then follow the instructions



Affect of Digital Signature and Encryption on Email Size





PII Breach Reporting Policy

- [DON CIO MESSAGE: DTG: 291652Z FEB 08](#)
 - DON PERSONNEL WHO HAVE DISCOVERED A KNOWN OR SUSPECTED LOSS OF PII MUST REPORT THE BREACH TO THEIR SUPERVISOR. COMMANDS/ACTIVITIES WILL DESIGNATE AN OFFICIAL IN THE CHAIN OF COMMAND RESPONSIBLE FOR REPORTING PII BREACHES AND TO SERVE AS A POINT OF CONTACT (POC) FOR FOLLOW-UP ACTIONS AND INDIVIDUAL NOTIFICATIONS.
 - PER REF B, THE TERM “BREACH” IS USED TO INCLUDE THE LOSS OF CONTROL, COMPROMISE, UNAUTHORIZED DISCLOSURE, UNAUTHORIZED ACQUISITION, UNAUTHORIZED ACCESS, OR ANY SIMILAR TERM REFERRING TO SITUATIONS WHERE PERSONS OTHER THAN AUTHORIZED USERS, FOR OTHER THAN AUTHORIZED PURPOSE, HAVE ACCESS OR POTENTIAL ACCESS TO PII, WHETHER PHYSICAL OR ELECTRONIC.
 - **WITHIN ONE HOUR OF THE DISCOVERY OF A LOSS OR SUSPECTED LOSS OF PII, NOTIFY VIA A SINGLE EMAIL THE FOLLOWING PRIVACY OFFICIALS AND AGENCIES OF THE LOSS:**
- DON CIO Resources:
 - [PII Breach Reporting Resources](#)
 - Automated reporting form
 - Sample notification letter
 - Breach consequences for military, civilians, and contractors



Myths Debunked

- **Sending a Digitally Signed email within the GIG provides the same protection as encryption.**
 - The GIG is not a secure environment. Only encrypted emails will provide reasonable assurance of confidentiality.
- **If you are having problems sending an encrypted email to someone, get them to send you an encrypted email.**
 - This may work, but only because the sender's email was also digitally signed.
- **Last four of a member SSN is not sensitive PII.**
 - According to the DON CIO, a member's SSN, in its full or truncated form, is sensitive PII.
- **A member can choose to transmit his/her own private information unencrypted.**
 - Policy does not exempt individuals from exposing their own personal information.
- **A member cannot send a digitally signed email or an encrypted email to a recipient outside of the GIG.**
 - Digitally signed email can be sent outside the GIG with no difficulty. Encrypted email can be sent outside the GIG as long as the sender has access to the recipient's public key, and this key is "trusted" by the sender.



Moving Forward

- If you are in the habit of sending sensitive information over email unprotected, STOP.
 - Use the “Ready... Aim... Fire” method
 - If you are having trouble sending encrypted email, conduct the misfire procedures. DO NOT get frustrated and just click send. If you can’t figure it out, get help from a coworker, contact your IAM, or call NMCI.
- If you send or receive an email containing sensitive information that was not encrypted, REPORT IT.
 - Notify your supervisor
 - Contact your Command Privacy Officer
- If you are a supervisor, send an encrypted test email to your subordinates on a periodic basis to ensure their certificates are published.

Slides 1, 18, and 19 have no notes.

Slide 2

- This slide is meant to show that clicking “send” on an email is just like pulling a trigger. Users need to realize that emails have the potential to cause damage; therefore, they must ensure not only that sensitive information is protected, but also that this information is sent only to those with a need to know.
- Understanding the Navy’s policy and how email works (specifically the difference between encryption and digital signature) should lower the potential for PII breaches.

Slide 3

This slide is meant to show that although email is like a loaded weapon that has the potential to cause damage, there are some “safeties” available to the user. This brief focuses on how these safeties work and when they should be used. The hope is that a better understanding of policy and email protection mechanisms will keep the Navy moving towards a culture that is more information protection conscious.

Slide 4

- The brief starts with the Navy’s policy on email encryption and digital signature, mostly to show under what circumstances they are required to be used and that information does not have to be PII to be sensitive.
- The next part of the brief examines encryption and digital signature to provide a better understanding of what they can and can’t do.
- Ready... Aim... Fire... is the biggest takeaway of this brief. Users need to treat email like a weapon system to help minimize the probability of exposing sensitive information.
- Frustration with encryption may be one reason why users do not like using it; therefore, the brief covers misfire procedures to help users overcome common encryption issues.
- Finally, PII breach procedures are communicated along with a slide showing how past breaches have impacted the NPC organization. The importance of “trust” in the organization cannot be overstated.

Slide 5

The requirement to encrypt sensitive emails has been around since 2004. It is interesting to note that the requirement applies not only to PII, but also other potentially sensitive information like contracting and OPSEC indicators. Another example could be pre-decisional materials that address controversial or sensitive issues (e.g., manning).

[R 071651Z DEC 04 CNO WASHINGTON DC:](https://infosec.nmci.navy.mil/PKI/R071651ZDEC04CNOWASHINGTONDCUNCLAS.pdf)

<https://infosec.nmci.navy.mil/PKI/R071651ZDEC04CNOWASHINGTONDCUNCLAS.pdf>

[NAVADMIN 248/08](http://www.public.navy.mil/bupers-npc/reference/messages/Documents/NAVADMINS/NAV2008/NAV08248.txt): <http://www.public.navy.mil/bupers-npc/reference/messages/Documents/NAVADMINS/NAV2008/NAV08248.txt>

[DON Digital Signature and Encryption Policy for Emails Containing PII](http://www.doncio.navy.mil/ContentView.aspx?ID=2451): <http://www.doncio.navy.mil/ContentView.aspx?ID=2451>

Slide 6

- Outlook uses both symmetric and asymmetric encryption techniques when encrypting email.
- An attachment does not need to be password protected if the email it is attached to is encrypted. Although okay to use for Office 2007 applications, password protected files introduce additional problems, like the need to send the password out-of-band. (Note: Office 2003 password protection has known vulnerabilities whereas Office 2007 uses a NSA approved encryption algorithm).

Slide 7

- Sensitive PII is a subset of unclassified, sensitive information.
- The FOUO marking is widely misused. There are nine exemption categories that stipulate what information may be marked FOUO, which protects the information from public release.

[DoD 5400.11-R](http://www.dtic.mil/whs/directives/corres/pdf/540011r.pdf) : <http://www.dtic.mil/whs/directives/corres/pdf/540011r.pdf>

[DoD 5200.1-R](http://www.dtic.mil/whs/directives/corres/pdf/520001r.pdf): <http://www.dtic.mil/whs/directives/corres/pdf/520001r.pdf>

Slide 8

- The DON makes a distinction between sensitive and non-sensitive PII (<http://www.doncio.navy.mil/contentview.aspx?id=2428>). Non-sensitive PII, like business email and business phone number, is releasable to the public and usually does not need to be protected or reported as a breach if “compromised.”
- Note: Last four is sensitive PII!
- Always consider the context of the information. If in doubt, encrypt!

Slide 9

Receiver/Sender

1. Before encryption will work, the recipient must publish his/her certificate to the GAL, or the sender must have the recipient’s certificate in his/her contacts list (which is accomplished by saving a contact from a digitally signed email). The recipient’s certificate contains his/her public key – this key is used in the encryption process.

Sender

1. The text of the email and any attachments comprise the message.
2. This message is encrypted using a randomly generated symmetric encryption key.
3. The randomly generated key is encrypted with the recipients public key.
4. Both the encrypted message and the encrypted symmetric key are grouped together to form an encrypted email.

Receiver

1. When the encrypted email is opened, its payload yields both the encrypted message and the encrypted symmetric key.
2. The encrypted symmetric key is decrypted using the receiver's private key. The private key is located on the receiver's CAC, and it can be used only if the PIN is known.
3. The encrypted message is then decrypted using the decrypted symmetric key that was randomly generated by the sender. Because only the recipient of the email possesses the corresponding private key of the public key that was used to encrypt the symmetric key (which was used to encrypt the message), we can reasonably conclude that the message is only accessible to the recipient (confidentiality).

Slide 10

Digital signature is not encryption. Digital signature only guarantees that the sender is who he/she claims to be and that the message was not modified in transit.

Slide 11

Sender

1. The text of the email and any attachments comprise the message.
2. This message of varying size is then passed through a hashing function. This one-way hashing function produces a fixed size output called a message digest. No matter what size the message, the message digest will always be a fixed length (for SHA-1, this length is 160 bits). Any change in the message will produce a dramatically different message digest. Note: a hash function is one-way because it is impossible to retrieve the original message from the fixed-bit output.
3. The message digest is encrypted with the sender's private key. The private key is located on the sender's CAC, and it can be used only if the PIN is known.
4. Both the encrypted message digest, the original message (which includes any attachments), and the sender's certificate (located on the sender's CAC) are grouped together to form a digitally signed email. This email can be delivered to any email account (government or private).

Receiver

1. When the digitally signed email is opened, its payload yields an encrypted message digest, the original message (which includes any attachments), and the sender's certificate. Note that the message and attachments are not encrypted and can be read by any recipient.
2. The certificate (which contains the public key) is validated via an Internet connection.
3. The encrypted message digest is decrypted using the sender's public key to produce the original message digest.
4. The original message and its attachments are passed through the same hashing function used by the sender, producing a message digest.
5. The decrypted message digest and the message digest created from the received email text and its attachments are then compared. If the message digests are identical, we can reasonably conclude that the message was not modified in transit (integrity). And, because we were able to validate the user's certificate and decrypt the message digest in the first place, we can reasonably assume that the message was indeed sent by the person who claimed to have sent the message (authentication) because only that person has access to his/her private key. For this same reason, the person who sent the message also cannot deny having sent the message (non-repudiation).

Slide 12

- The biggest takeaway from this brief is Ready... Aim... Fire! - It is an easy to remember method to check each email before clicking send.
- Also discussed on this slide are marking requirements. Marking email subject lines, the message body, and filenames with FOUO alerts the recipient that the email/file contains sensitive information.
- Users need to be confident that recipients selected from the GAL are indeed the correct persons and that these persons have a "need to know."

Slide 13

The reluctance to use encryption may be partly due to the occasional issue encountered when trying to send encrypted email. This slide provides step-by-step procedures of how to deal with these problems.

Slide 14

- After verifying the recipient's certificates are valid, and an encrypted email still cannot be sent, downloading the full details of the address book may solve the problem. Downloading the address book will take about 5-10 minutes.
- "Cached Exchange Mode" can also cause encryption problems. Deselecting this mode has proved to allow encrypted emails to be sent in some cases.

Slide 15

- Investigate invalid digital signatures since the email may have been spoofed by a third party or the information could have been modified in transit.
- Also, if opening an old email, be aware that the digital signature may no longer be valid if the certificate has expired. The email was probably valid when it was originally transmitted.
- If you cannot open an old encrypted email, more than likely you are now using a newer public-private key pair than what was used when the older email was transmitted. If this is the case, all you need to do is recover your older private key from an escrow account maintained at DISA. This task can be accomplished by visiting the website on the slide, selecting the older certificate (look at the date range to see which one you need), and then follow the instructions.

Slide 16

- One challenge with sending digitally signed and encrypted email is dealing with the fact that the email size will grow due to how the message is stored (go to <http://support.microsoft.com/kb/927092> to read Microsoft's explanation of this phenomenon).
- Digitally signing or encrypting an email will increase its size by 4/3 (33%, not including other overhead).
- Digitally signing and encrypting an email will increase its size by 16/9 (78%, not including other overhead).
- Since it is Navy policy to digitally sign any email with attachments, a large email size due to both digitally signing and encrypting is a probable occurrence.

Slide 17

- The requirement to report the potential compromise of PII is well known; however, it is not well known that the breach reporting policy also applies to sent unencrypted email containing PII.
- Sending email containing sensitive PII (encrypted or unencrypted) to a person that does not have a need to know (i.e., the information is not needed in the performance of assigned duties) also constitutes a breach, regardless of the position, rank, or clearance of the recipient.
- All breaches must be reported, but the process needs to include the Chain of Command and the IAM. The decision to send out notification letters to affected members will be adjudicated at the DON CIO and communicated to the command.

[DON CIO MESSAGE: DTG: 291652Z FEB 08](http://www.doncio.navy.mil/Download.aspx?AttachID=470): <http://www.doncio.navy.mil/Download.aspx?AttachID=470>

[PII Breach Reporting Resources](http://www.doncio.navy.mil/ContentView.aspx?id=852): <http://www.doncio.navy.mil/ContentView.aspx?id=852>