



DEPARTMENT OF THE NAVY  
BUREAU OF NAVAL PERSONNEL  
5720 INTEGRITY DRIVE  
MILLINGTON, TN 38055-0000

BUPERSINST 5230.9  
BUPERS-07  
**1 6 FEB 2012**

BUPERS INSTRUCTION 5230.9

From: Chief of Naval Personnel

Subj: USE OF EMAIL DIGITAL SIGNATURE AND ENCRYPTION AND THE  
REPORTING OF AN EMAIL BREACH OF SENSITIVE INFORMATION

Ref: (a) DoD 5400.11-R of 14 May 2007  
(b) CNO WASHINGTON DC 071651Z Dec 04  
(c) DON CIO WASHINGTON DC 032009Z Oct 08  
(d) DON CIO WASHINGTON DC 291652Z Feb 08

Encl: (1) Sensitive Information, Sensitive PII, and Non-  
sensitive PII  
(2) Sensitive Information Breach Reporting Requirements  
(3) Printable Reference and Troubleshooting Guide

1. Purpose. Reference (a) describes the Department of Defense Privacy Program. References (b) and (c) establish and expand upon Department of Navy (DON) policy regarding the use of digital signature and encryption, and reference (d) outlines the procedures for reporting a personally identifiable information (PII) breach. The purpose of this instruction is to provide Bureau of Naval Personnel (BUPERS) clarification and execution of these existing policies to ensure the protection of unclassified, sensitive information sent via email.

2. Background. Digital signature and encryption are two separate and distinct mechanisms that can be used to protect email. Digital signature is used to provide reasonable assurance that the message was sent by the person who claimed to have sent it (authenticity) and that the message was not modified in transit (integrity). A person also cannot deny having sent a digitally signed message (non-repudiation). Encryption is used to provide reasonable assurance that a message cannot be opened by anyone but the intended recipient(s) (confidentiality). This policy helps users identify under what circumstances email must be digitally signed, encrypted, or both, and what actions to take if unclassified, sensitive information is transmitted negligently (i.e., unencrypted).

3. Applicability. This policy applies to all members of BUPERS commands (military, civilian, and contractor) who send emails to or from unclassified, government provided email accounts. Additionally, this policy applies to all emails sent from any platform utilizing a government email account (e.g., government provided workstations, personal digital assistants (PDAs) (e.g., BlackBerries), or Outlook Web Access (OWA)).

4. Policy. All members of BUPERS commands will adhere to the following digital signature, encryption, and reporting requirements.

a. Digital Signature shall be used when transmitting emails containing official business, attachments, or clickable links.

b. Encryption shall be used when transmitting emails containing unclassified, sensitive information. (Note: the difference between sensitive and non-sensitive PII is defined in enclosure (1)).

c. The reporting requirements outlined in enclosure (2) shall be followed immediately upon the discovery of a breach of sensitive information.

5. Responsibilities

a. Commanders, Commanding Officers, and GS Equivalent

(1) Shall personally adhere to digital signature and encryption policy.

(2) Shall ensure digital signature and encryption requirements are understood and practiced within their organizations.

(3) Shall ensure the reporting requirements outlined in enclosure (2) are well known, understood, and executed in a timely manner in the event a breach occurs.

b. Command Information Officers, Command Information Assurance Managers, Command Privacy Officers, and Equivalent

(1) Shall personally adhere to digital signature and encryption policy.

(2) Shall coordinate to assist in educating the members of their respective commands in the proper use of digital signature and encryption, and what actions to take if they discover an unencrypted email containing unclassified, sensitive information.

c. All Users

(1) Shall adhere to digital signature and encryption policy.

(2) Shall ensure valid certificates are published to the Global Address List (GAL) to facilitate encrypted email communications.

(3) Shall use diligence and good judgment when transmitting sensitive information via email.

(4) Shall report the discovery of a sensitive PII breach in accordance with the requirements outlined in enclosure (2).

6. Points of Contact. BUPERS Information Assurance Manager, (BUPERS-073); BUPERS Command Privacy Officer, (PERS-00J6); and BUPERS Command Security Manager, (PERS-534).

7. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed per Secretary of the Navy (SECNAV) Manual M-5210.1 of November 2007.

8. Reports. Reporting requirements contained in this instruction are exempt from reports control per SECNAV Manual M-5214.1 of December 2005.



C. A. COVELL  
Rear Admiral, U.S. Navy  
Deputy Chief of Naval Personnel

Distribution:  
Electronic only, via BUPERS Web site  
<http://www.npc.navy.mil>

1 6 FEB 2012

**SENSITIVE INFORMATION, SENSITIVE PII, AND NON-SENSITIVE PII**

**Sensitive Information:** Emails containing sensitive information in the message body or in the attachments must be encrypted per reference (a). Unclassified, sensitive information include Privacy Act information, Health Insurance Portability and Accountability Act (HIPAA) information, contact information, for official use only (FOUO) information, and information that may serve as an operations security (OPSEC) indicator. Other examples of unclassified, sensitive information may include vendor proprietary information, pre-decisional materials, and any other unclassified information deemed sensitive in the context of the examples provided above. (Note: classified information shall only be transmitted on approved classified systems; the presence of classified information on an unclassified system constitutes a classified spillage, whether the information is encrypted or not.)

**Sensitive PII:** Emails containing sensitive PII in the message body or in the attachments must be encrypted. Examples of sensitive PII elements include, but are 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.

16 FEB 2012

**Non-Sensitive PII:** Emails containing non-sensitive PII in the message body or in the attachments usually do not need to be encrypted. According to the DON Chief Information Officer (CIO), examples of non-sensitive PII elements include, but are 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.

**Important Note:** Always consider the context of the information to determine whether or not the email should be encrypted. If in doubt, encrypt!

**SENSITIVE INFORMATION BREACH REPORTING REQUIREMENTS**

In the event of a breach or suspected breach, follow the procedures outlined in the questions below as soon as possible:

1. Is the suspected sensitive information classified?  
**Yes:** Notify the sender and contact your supervisor, your command security manager (CSM), and your command information assurance manager (IAM) immediately.  
**No:** Go to question 2.
2. Does the suspected sensitive information contain PII?  
**Yes:** Go to question 3.  
**No:** Go to paragraph 5.
3. Is the PII sensitive? (see enclosure (1))  
**Yes:** Go to paragraph 4.  
**No:** If the PII is not sensitive, no further action is required; however, if you believe the non-sensitive PII is sensitive in the context in which it was used, go to paragraph 4.
4. If the email was not encrypted or the recipient did not have a need to know (even if encrypted), contact your supervisor, your command IAM, and your command privacy officer. Your privacy officer will determine whether or not a formal report needs to be submitted to the DON CIO (note: the initial report needs to be submitted within 1 hour of discovery). Regardless of whether a formal report needs to be submitted, a sensitive PII breach also needs to be reported to the organization's commanding officer via the applicable chain of command.
5. Contact your supervisor and your command IAM to help determine whether the information is indeed sensitive and what course of action should be taken. Courses of action can range from a friendly email to the sender reminding him/her to encrypt sensitive information to contacting the sender's supervisor or commanding officer if the violation warrants higher visibility.

## PRINTABLE REFERENCE AND TROUBLESHOOTING GUIDE

### Command Contact Info

Command Privacy Officer:

Command Security Manager (CSM):

Command Information Assurance Manager (IAM):

---

Follow this procedure to publish your certificates:

- **Outlook: Tools -> Trust Center -> E-mail Security -> Publish to Global Address List (GAL)**

When sending emails, use the Ready... Aim... Fire! method.

- **Ready:** Draft email, select attachments, digitally sign (if not already selected), and encrypt (if required).
- **Aim:** If the email contains sensitive information, ensure the recipients selected have a need to know.
- **Fire:** Click "Send"

If email failed to send due to "Encryption Problems," follow "misfire" procedures below:

- DO NOT select "Send Unencrypted." Select "Cancel" and remove failed recipient addresses from the email, then click "Send."
- For NMCI recipients, send a separate email to unsupported email addresses requesting a reply with a digitally signed email after publishing their certificates to the GAL using the above procedure. Published certificates may not be available for a few minutes while NMCI servers replicate and or if the user's GAL is not synced. To manually sync GAL, follow this procedure: **My Computer: System (C:) -> Program Files -> Microsoft Office -> GlobalDirectory -> GALSyncU.exe**. Attempt to send encrypted email again.
- For non-NMCI recipients, send a separate email to unsupported email addresses requesting a reply with a digitally signed email. Right-click on the name in the email and select "Add to Outlook Contacts" then click "Save & Close." Attempt to send encrypted email again.

If encryption problems are still encountered, try one of the following:

- Go to the Outlook toolbar and click on the small arrow next to the "Send/Receive" button, then download the address book with "Full Details" (may take 5-10 minutes). Attempt to send encrypted email again.
- Using "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 -> Change (on Email tab)**. If "Cached Exchange Mode" 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).
- If still unable to send an encrypted email, contact the NMCI helpdesk.