Cyber Security Awareness

1.

USB Devices (Phones/ Memory Sticks/ iPods/Cameras)

- DO NOT plug them into USCG devices, workstations or docking stations. Not even to CHARGE!

2.

SENSITIVE INFORMATION (S-PII/PII/FOUO)

- DO NOT share with personnel lacking need to know
- Protect with lock and key when not in use

3.

EMAIL SECURITY

- If during the course of official duties you need to send FOUO information outside of the .mil network, then you need to take steps to protect from unauthorized disclosure. Acceptable steps include:

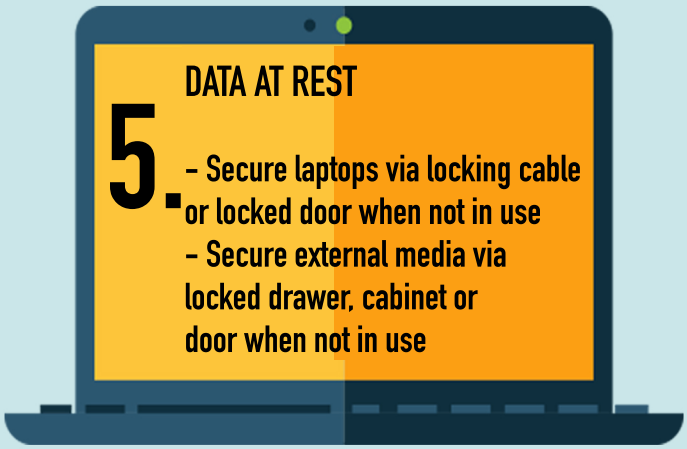
a) Encrypting the entire message
b) Encrypting as an attachment
c) Using an approved file transfer utility such as:
https://safe.amrdec.army.mil/safe/welcome.aspx

4.

CAC – Common Access Cards

- DO NOT leave unattended. CACs found in unattended workstations are subject to seizure and constitute a Cyber Security Infraction.

5.



DATA AT REST

- Secure laptops via locking cable or locked door when not in use
- Secure external media via locked drawer, cabinet or door when not in use

6.

PASSWORDS

- Never share
- DO NOT write down and attach to sticky notes or hide under keyboards or telephones

7.

USE of REMOVABLE MEDIA

-Only commercially produced CDs, DVDs or Government owned CD/DVD recordables are authorized for use
-Only approved encrypted hard drives

8.

BURN BAGS

- DO NOT leave burn bags unattended
- Any material found in a burn bag is considered FOUO, so don't treat them as recycle bags