Print Form | Save As | E-mail

U.S. Army Corps of Engineers (USACE)

CYBER SECURITY QUICK REFERENCE CARD

Post this Information at all computer workstations/work areas

For use of this form see AR 25-2, DoDI 5200.48, and SF 901; The proponent agency is CEIT-CS.

DO NOT LEAVE YOUR CAC UNATTENDED!

Display your CAC or badge visibly, above the waistline while on-site, or follow your local security policy (if different)

SUSPICIOUS EMAIL/SPAM

If you receive any suspicious email, phishing, or spam, DO NOT open attachments or click on any links.

Report immediately! **Contact the ESD and send an email to: SPAM-ReportToIronPort (in the GAL)**

Downloading unauthorized software is prohibited.

USEFUL INFORMATION

- Logoff, but do not shut off the computer to ensure patches are received.
- If traveling, ensure you connect to the network via VPN periodically so your laptop can receive patches.
- External hard drives and media need to be properly marked with classification.
- Unencrypted Personally Identifiable Information (PII) from/to commercial email will be detected and treated as a violation.
- Personally owned devices should **NOT** be connected to Government systems --**NOT EVEN TO CHARGE!**

COVER OR DISABLE YOUR CAMERA

External camera: cover the camera lens using a built-in camera cover, **or with paper**, OR physically unplug the camera from your computer.
Built-in camera: **use the built-in camera cover**, obtain a stick-on sliding camera cover, or with paper.
Do not cover the lens with tape or the sticky part of post-it. It may affect the lens.

DO NOT leave sensitive or PII documents on desks, printers, or in plain sight. Use cover sheets or lock in drawers/cabinets when not in use.

HOW TO PROTECT CUI/PII EMAIL

Ways to protect emails containing Controlled Unclassified Information (CUI) and PII:

1. Put "CUI" in the subject line and body of the email. *
2. The email must be digitally signed.
3. The email must be encrypted before sending.
4. Send the email only to recipients with a "need to know".

*CUI email marking information is at the following URL
https://www.archives.gov/files/cui/documents/cui-email-marking-tip-20180605.pdf

IMPORTANT CONTACT INFORMATION*

Enterprise Service Desk (ESD): (866) 562-2348

Your Information System Security Officer (ISSO)

Primary: _____

Backup: _____

Your Traditional/Physical Security Manager

Primary: _____

US Army Corps of Engineers

VIRUS/NETWORK ATTACK SYMPTOMS

- Request to provide, reset or change password
- Email from unfamiliar source (see Suspicious Email / SPAM section)
- Notification of login attempts by an unknown user
- Unexplained inability to log on
- Unexplained modifications/deletion of data/error messages
- Denial of service (e.g., information being held ransom)
- Sudden lack of hard drive space
- Computer continually restarts
- **Out-of-memory error messages (PC with sufficient RAM)**

COMPUTER VIRUS REPORTING PROCEDURES

STEP 1: Disconnect the network cable then **disable** the wireless connection and stop using the computer.

STEP 2: Leave the system powered up!
Do not click on any prompts, close any windows, or shut down the system.

STEP 3: Document the following:
- Actions prior to virus
- Any error messages that appeared
- Event date and time

STEP 4: Report immediately to the ESD!

DO NOT discuss/transmit classified information via non-secure means!

CLASSIFIED MESSAGE INCIDENT (CMI)

CMI Overview

A CMI or spillage occurs when a higher classification level of data is transferred to a lower classification level system/ device. **Report any unauthorized USB or wireless devices inside the Classified Processing Area(s).**
CMI / spillage requires immediate response.

CMI Response

1. **Disconnect the** network cable then **disable** the wireless connection and **stop using the computer.**
2. **Do not power down or log off.**
3. **Do not forward, print, or delete messages.**
4. Immediately contact the ESD, your ISSO, and your Security Manager. Provide them:
   - Event date/time
   - Name of POC
   - Location of system
5. Do not discuss the content of classified information over unclassified communication. Provide only unclassified information to assist with Incident Response actions.
6. Isolate all external media used (e.g., disks or CDs)
7. **Do not** leave the computer unattended. The person protecting the computer should be cleared to the level of the message.

PHYSICAL SPACE REQUIRED FOR CLASSIFIED SYSTEMS

Device / Equipment Type	Distance	Distance in inches
Unclassified to Classified	0.5 meters	20 inches
Classified to Classified	0.5 meters	20 inches

CONTACT Asset Management / ULA before moving any Government Computer Equipment!

***Contact information as of:** _____