Cyber Security Tips

- **Refresh your knowledge of cybersecurity** by completing the Annual Cyber Awareness training: https://cs.signal.army.mil/
- **No cell phones in areas with classified systems. Classified monitors must face away from windows if not covered with blinds or curtains.**
- **Do not connect personally owned equipment (i.e., personal cell phones, personal or contractor issued computers, thumb drives, SD cards or other personal electronic devices) to the DoD network.**
- **Downloading unauthorized software to the DoD network is strictly prohibited**.
- **Keep your Common Access Card (CAC) in your possession at all times.** When you leave your computer unattended, you must remove and take your CAC with you.
- **Personally Identifiable Information (PII)- Do not reply to spam emails** or reveal personal information such as your DOB, SSN or credit card information to unknown sources. This could result in your identity being stolen and used for illegal purposes. **When in doubt always encrypt and digitally sign all PII, OPSEC, medical, and/or contract sensitive data**.

Contact your ISSM or Security Manager for all Cyber Security issues.

Contact Information

HOURS OF OPERATION:
Mon - Fri 0700-1700 Hours
Excludes Federal Holidays

Mid-Atlantic Region Information Systems Security Manager (ISSM)
Mr. Alton J. Thompson
alton.j.thompson.civ@army.mil
(410) 279-2228

MAR Traditional Security (TRADSEC)
Mr. Jeffrey R. Lopus
jeffrey.r.lopus.civ@army.mil
(410) 278-9628

MAR Cyber Incident Response Team (CIRT)
Mr. Peter D. D'Amico
Mid-Atlantic Region IRT Email:
usarmy.apg.NETCOM.mbx.iad-csirt@army.mil

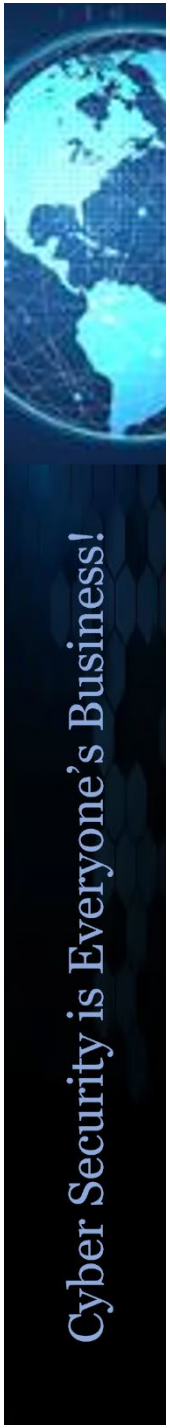
***** APG Cyber Security Hotline*****
(410) 306-3700
Note: Please use for Cyber Security incident reporting only

Available Resources:

Fort Gordon Cyber Training Center
https://cs.signal.army.mil/

Cyber Security Technical Implementation Guides (STIG)
https://cyber.mil/stigs

Cyber Security is Everyone's Business!



MID-ATLANTIC REGION
NETWORK ENTERPRISE CENTER
(MARNEC)
CYBER SECURITY DIVISION

CYBER COMMAND READINESS INSPECTION (CCRI)

A User's Guide

Virus Infection/Suspicious Events

If you notice your computer is:

- Running slower than usual
- Displaying odd error messages
- Suddenly out of space
- Unable to save files
- Pulling up corrupt files
- Missing recently used software or files
- Freezing often and has to be restarted
- Opening and closing the CD-ROM tray by itself
- Launching programs on its own
- Playing unusual sounds randomly

… Your computer may be compromised. Complete the following actions:

Do:

- Notify your IMO or ISSM
- Write down any errors that you see
- Unplug the network cable
- If chain of command is not available contact the IRT.

Do not:

- Turn off your computer
- Send any email
- Delete any files

Never open email or attachments from Unknown from unsolicited sources.

NDCI

A Negligent Discharge of Classified Information (NDCI) occurs when classified data is found on a system accredited for a lower classification.

Example: A SECRET document found on Unclassified Network (NIPRNet).

If a NDCI has occurred:

Do:

- Cease all work on the affected system, printer or MFD
- Turn off the monitor
- Unplug the network cable
- Notify your IMO and S6
- Contact the IRT
- Have someone with the appropriate clearance physically guard the system

Do not:

- Leave your computer unattended
- Turn off your computer
- Send any email
- Delete any files
- Discuss details of the incident over unsecure communications

Check with your ISSM or ISSO to ensure that all devices are labeled with the correct classification.

NDCI Checklists shall be filled out & submitted on classified network. If CONFIDENTIAL or SECRET involved, use SIPRNET.

Traditional Security (TRADSEC) Tips

For security containers (safes), PDS drop boxes, and vault doors, you must use the SF700 form to record the combination. The SF701 Activity Security Checklist is used for end of day security checks, and the SF702 Security Container Check Sheet is used when opening/ closing/ verifying security of each item.
Contact your G2 / S2 / Security Manager if you have questions about SF700, SF701, or SF702 forms.

Ensure security containers are CLOSED and SECURED whenever left unattended and checked as required for your area.

If you are working in an approved **'Open Storage'** area, keep in mind that only approved items on the open storage memorandum can be left out unattended. All other classified items must still be secured when the space is left unattended.

For **'attended processing'** (closed storage) areas, ensure the TACLANE crypto key, SIPR SWITCH, and any other classified items are secured in a safe when unattended.

Ensure access rosters are signed by the proper signature authority and have current personnel listed.

Finally, ensure everyone in your office understands the security procedures for the area.

If you have questions concerning TRADSEC, please contact your S2/S6 representatives or the MARNEC TRADSEC team.