DEPARTMENT OF THE NAVY
CHIEF OF NAVAL AIR TRAINING
250 LEXINGTON BLVD SUITE 102
CORPUS CHRISTI TX 78419-5041

5510
Memo 00/452
10 Jul 2018

MEMORANDUM FOR DISTRIBUTION

From: Chief of Naval Air Training

To: All Hands

Subj: COMMON ACCESS CARD AND PERSONAL ELECTRONIC DEVICE REQUIREMENTS FOR CHIEF OF NAVAL AIR TRAINING AND SUBORDINATE COMMANDS

1. Fleet Cyber Forces Command (FLTCYBERCOM) conducted a Command Cyber Readiness Inspection (CCRI) on Chief of Naval Air Training (CNATRA) from 25 to 29 June 2018. Inspection results noted several discrepancies that need to be addressed immediately in regards to CNATRA Headquarters and Naval Air Training Command (NATRACOM) Cyber Security Culture.

2. All CNATRA and NATRACOM Personnel (Military, Civilians, and Contractors) will adhere to Cyber Security policies, directives and best practices at all times. If you notice an unattended Common Access Card (CAC) you are not allowed to remove it. Contact the Military Member/Employee's Supervisor and the responsible Command Security Manager immediately.

Actions you should take to safeguard your CAC:

a. Maintain control of your CAC/Military Identification (ID) at all times.

b. Remember to remove your CAC from your computer when you leave your desk.

c. Do not display your CAC or any other credentials that contain Personally Identifiable Information (PII) when you leave the workplace. For example, do not have your CAC/Military ID visible while riding public transportation.

d. Except for Department of Defense (DoD) health care providers, do not allow organizations/businesses to reproduce (photocopy, scan, or other means) an image copy of your CAC/Military ID. If you know of a non-medical organization possessing an image copy of your CAC/Military ID, request destruction of the image.

e. In the event a CAC scan application comes into the market, do not attempt to use or test it on your mobile device, as the barcode information may be sent to an unknown server, stored, and made available for public release.

may only be used in the event government provided services are not available and must be authorized in writing by the first Flag Officer in the Chain of Command. PEDs are not authorized to be connected to government computer systems. Unauthorized devices are detected by automated computer security systems. These connections are blocked, but will trigger a computer security incident.

4. Cyber Security is everyone's responsibility. Unit Commanders are directed to brief this information to all hands immediately and implement measures to ensure 100% compliance with all DoD/Department of the Navy (DON) policies and directives.

J. S. BYNUM

Copy to:
CNATRA Website