☑ If you have a **security container, PDS Drop Box, or a Vault Door** you must record the combination on an SF 700 . Part 1 of the SF 700 contains names and contact info for who has the combination to the safe. Part 1 is U//FOUO and must be stored in an **envelope inside of each safe, PDS drop box and vault door.** Part 2 of the SF 700 contains the actual combination to the security container. It must be stored in an S2 safe in your unit. The cost for drilling safes, when no one knows the combination is $2300, as of March 2015. Please ensure you record combinations to avoid unnecessary costs to the government!

☑ For your security containers, PDS Drop Boxes and Vault Doors, you must use a SF 701 Activity Security Checklist, and use the SF 702 Security Container Check Sheet. It is each user's responsibility to ensure correct use of these forms.

Contact your G2/S2 if you have questions about SF 700, SF 701 or SF 702 forms.

☑ Do not tape/stick anything to your safe. Put the SF 702 on the top or behind the open/closed magnet. There should be NOTHING on top of your security container.

☑ Each unit/element or section bears the responsibility to keep classified holdings to the minimum level needed to accomplish their respective missions. RNEC-NCR custodians of classified information should conduct **a 100 percent systematic review of all classified material quarterly.**

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

☑ If you are working in an approved 'Open Storage Area' (OS)– be aware of what exactly that means. When you leave your OS area, ALL printed Classified, Classified CDs, classified laptops and classified hard drives must be **LOCKED in a Security Container!! (Even in OS Approved Areas!)**

Exactly what is approved to be left out (generally equipment that does NOT fit in a safe) will be specified in your OS Approval.

Contact your G2/S2 if you have questions about Open Storage.

☑ If your office / building has a Protected Distribution System (PDS) – which is used to distribute SIPRnet throughout your building, ensure that the PDS is visible (don't block it with furniture, etc.) Also, do not attach anything to the PDS, and the PDS cannot be painted. Each PDS must have a SF 702 and be checked daily, and have a S&G 8077 or NSA Tamper Evident padlock. The lock must be secured when not in use. The entire PDS of each building must be checked daily, for signs of tampering. The Staff Duty Officer must have the appropriate security clearance, be trained and appointed in writing to check the PDS.

Contact your G6/S6 if you have questions about your PDS.

☑ Ensure online Security Awareness and Refresher Training Records are up to date, as these may be inspected.

☑ Ensure access rosters are signed and have current personnel listed.

☑ Remember that classified material must always be under your direct control. If you are the last person to leave your area, do not leave classified materials unattended! Secure all classified material in a GSA approved security container and secure your PDS box / vault door as required.

☑ Finally, ensure that everyone in your office knows and understands the security procedures for the area.

If you have any questions, please contact your local S6 / S2 team. If you still have questions, please contact the respective RNEC/LNEC POC below.

RNEC NCR POCs:
TRADSEC- Janet Geisler 703.704.1007/Wilson Trapp 703.704.3063
RNEC Security Managers- Stacey Wrin 703.704.4457 /Mason Haynesworth -703.704.4754
Regional ISSM - David Morris 703.704.4151
RNEC Belvoir Cyber Chief - Maria I Nelson 703.704.1933
LNEC JBMHH - Calvin Taylor 703.696.3979
LNEC Meade - Bernardo Perdomo 301.677.1611
LNEC APHill - Robert Warden 804.633.8350

COMMAND CYBER READINESS

Pre-Inspection = 25 FEB -8 MAR 2019

Command Cyber Readiness Inspection = 17-27 JUN 2019

WHAT EVERY SOLDIER, CIVILIAN, AND CONTRACTOR CAN DO TO COMPLY WITH CYBER SECURITY REQUIREMENTS

JAN 2019

What is the CCRI?

The Command Cyber Readiness Inspection (CCRI) is a thorough review of a Department of Defense entity's cyber-readiness status conducted. The criteria for the review are based on several key industry standards, including DISA's Security Technical Implementation Guides (STIGs), and various Chairman of the Joint Chiefs of Staffs Instruction (CJCSI) and Army directives.

Much of the CCRI will focus on the Network Enterprise Center (NEC) and how the systems are configured, but a portion of the CCRI will look at **security at units and individual user levels**. If your area has **active SIPRNet**, there is a **HIGH Probability** that the CCRI team will be in your area to inspect. This is where we need the Security Managers, supervisors and every computer user's assistance.

Inspectable Areas

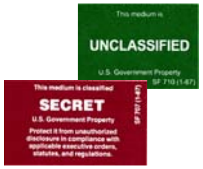
Inspectors may look at **all workspaces on all installations** using the DISA Traditional Security Checklist, Version: 1, Release: 2, dated 24 Jul 2013 as their basis. This brochure identifies the common Traditional Security discrepancies, found during the CCRI Staff Assistance Visit in February 2016, and should be used as a guide to ensure your area is prepared for the actual CCRI.

How can you help?

☑ **Make sure to remove CACs and SIPR tokens when stepping away from your computer!**

EVERY INSTANCE of a CAC / SIPR token in a computer will count as a **CAT 1 Finding**. CAT I Severity Code is assigned to findings that allow primary security protections to be bypassed, allowing immediate access by unauthorized personnel or unauthorized assumption of super-user privileges. During the CCRI, the **NAME** all individuals whose CACs / SIPR tokens are found unattended will be briefed to the **CG during the inspection out-brief**.

☑ Ensure all NIPR and SIPR computers, printers, digital senders, etc. in your area are marked with classification stickers. **If you need stickers, contact your G2/S2.**



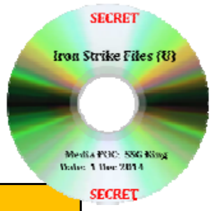
This medium is
UNCLASSIFIED
U.S. Government Property
SF 710 (1-87)

This medium is classified
SECRET
U.S. Government Property
Protect it from unauthorized disclosure in compliance with applicable executive orders, statutes, and regulations.
SF 707 (1-87)

☑ Ensure your shredder bags are no more than ½ full. There must be an NSA approved shredder in all spaces with classified printers with the proper FORSCOM Poster 139-R conspicuously placed on the units.

☑ Label CDs/DVDs properly:
(Use a Sharpie, NOT stickers)

- Classification on top & bottom
- Title (w/classification)
- Media POC
- Date CD/DVD was made

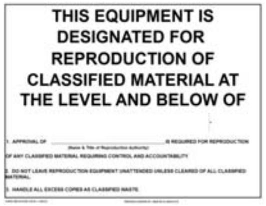


MARKINGS ARE FOR EXAMPLE PURPOSES ONLY

SHRED CDs/DVDs when NO LONGER NEEDED.

Classified CDs are NOT AUTHORIZED to be stored anywhere but in a SECURITY CONTAINER. Even if your area is approved for Open Storage of Classified, **CDs must be stored in a security container when not in use.**

☑ Ensure the FORSCOM Form 138-R is completed and conspicuously placed on or near each item of equipment authorized for reproduction of classified information. (for all areas where classified is processed)

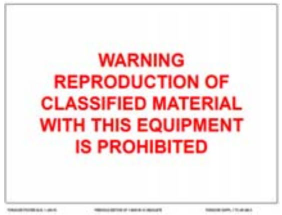


THIS EQUIPMENT IS DESIGNATED FOR REPRODUCTION OF CLASSIFIED MATERIAL AT THE LEVEL AND BELOW OF

1. APPROVAL OF ______ IS REQUIRED FOR REPRODUCTION
(Name & Title of Reproduction Authority)
OF ANY CLASSIFIED MATERIAL REQUIRING CONTROL AND ACCOUNTABILITY

2. DO NOT LEAVE REPRODUCTION EQUIPMENT UNATTENDED UNLESS CLEARED OF ALL CLASSIFIED MATERIAL

3. HANDLE ALL EXCESS COPIES AS CLASSIFIED WASTE



WARNING
REPRODUCTION OF CLASSIFIED MATERIAL WITH THIS EQUIPMENT IS PROHIBITED

☑ Ensure the FORSCOM Poster 93-R is conspicuously placed on all reproduction equipment to clearly indicate that reproduction of classified information is prohibited.

☑ In areas with NIPR and SIPR, users must make sure that their computers / printers / cables, etc. maintain correct separation distances:

Classified------------------3 Feet---------------Unclassified
Computer / Printer   Computer / Printer

Classified-------------------2 in-----------------Unclassified
Cat 5/6 Cable   Cat 5/6 Cable

(No separation required for fiber and there is no such thing as RED/RED separation, so your SECRET and TOP SECRET systems can be right next to each other.)

Consult your G6/S6 if you have questions about separation distances.

☑ Cordless phones are **NOT authorized in ANY Office Space.**

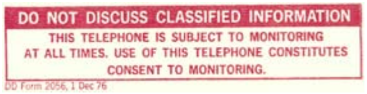
☑ Wireless mice are **NOT authorized in any Office Space.**

REMOVE THESE ITEMS FROM YOUR WORK AREAS.

☑ Ensure users do not use personal electronic devices within 10 feet of active SIRPNet or classified processing equipment. **This includes any 'approved' / DoD issued Blackberry Devices.**

NO ELECTRONIC DEVICES ALLOWED BEYOND THIS POINT

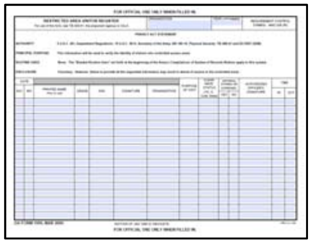
☑ Ensure DD Form 2056 consent to monitor labels are on all phones.



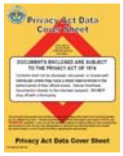
DO NOT DISCUSS CLASSIFIED INFORMATION
THIS TELEPHONE IS SUBJECT TO MONITORING AT ALL TIMES. USE OF THIS TELEPHONE CONSTITUTES CONSENT TO MONITORING.
DD Form 2056, 1 Dec 76

For S-VoiPs, you may cut off the top portion of the DD Form 2056, but there still must be a consent to monitoring sticker on every phone.

☑ Ensure visitors are signed in, if required for your work area if you have a secure room or Open Storage Area. Remember to ask visitors if they have electronics and ask that they be secured outside of your area. Use a DA Form 1999 to sign in visitors.



☑ Use a PII Coversheet to protect Privacy Act Data. Store PII in a **locked drawer/ cabinet when not in use.** Put a PII Coversheet on the drawers of cabinets containing PII. ENSURE drawers containing PII ARE LOCKED and THE KEY IS IN ANOTHER LOCATION (lock box, locked drawer) or in the possession of a designated person with a need to know. If you have a lock box, the lock box must not have the key to the lock box in the lock box.



Privacy Act Data Cover Sheet
DOCUMENTS ENCLOSED ARE SUBJECT TO THE PRIVACY ACT OF 1974
Privacy Act Data Cover Sheet