



DCOMD NORAD CFSU (CS) & Dets

UNIT COMCO

23 Sep 2025



CAN UNCLASSIFIED

COMCO References

NDSODs – [National Defence Security Orders](#) (French Available)

CSS 100 – [Canadian Signal Intelligence Security Standards](#) (English Only)

CTSS 100 – [Canadian Talent Keyhole Security Standards](#) (English Only)

CTSI 100.4 – [Marking and Handling Policy](#) (English Only)

CTSI 100.5 – [Personnel Access Policy](#) (French Available)

CTSI 100.8 – [Unit COMCO Duties & Responsibilities](#) (English Only)

- [NSC Sharepoint Site](#) (French Available)
- [CANELEMNORAD Security](#) (French Available)

[++CANELEMNORAD COMCO – OCIC CANELEMNORAD@CANELEMNORAD DCOMD
NORAD@COLORADO SPRINGS, US](#)

CANELEMNORADCOMCO-OCICCANELEMNORAD@forces.gc.ca

CAN UNCLASSIFIED



CAN UNCLASSIFIED

COMCO Duties & Responsibilities

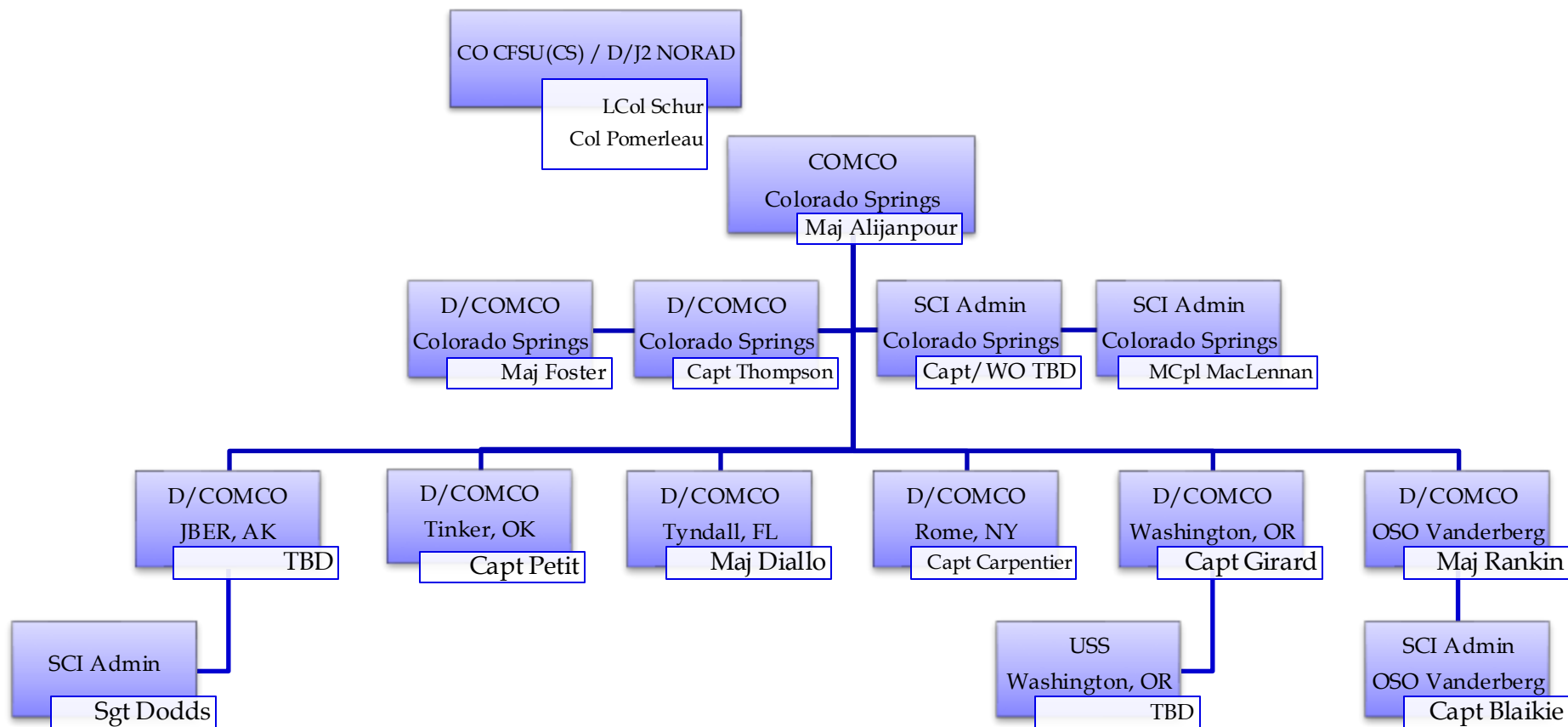
- The Unit COMCO is responsible for all aspects of TK security including:
 - Protecting TK Material in the workplace; (Material Handling, Advise on Security Matters)
 - Enforcing Personnel Security Standards; (Manage TK access, Indoc/De-Indoc, Change of Circumstances)
 - Enforcing Physical Security Standards; (SCIF Accreditation, Access, and Security)
 - Managing Non-compliance. (Security Event/Incident Management)
- The Unit COMCO is officially appointed by the Authorized Organization's CO.
 - Seconded by Deputy COMCOs (Can fulfill the same responsibilities as UNIT OMCO)
 - Aided by SCI Administrators (Limited to SCI requests and Indoc/De-Indoc)
- COMCO answers to Unit CO and NSC.
 - NSC is responsible to TCO CAN (Comd CFINTCOM)
- COMCO team members should attend and successfully complete the ALMG – Unit COMCO Course.
- Unit COMCO is not a USS and prohibited to fulfill both roles by national policy.

CAN UNCLASSIFIED



CAN UNCLASSIFIED

DCOMD NORAD COMCO Framework





CAN UNCLASSIFIED

OUTCAN SCI Requests

COMCO

- Reception of Screening or Posting Message;
- Verify Positional Requirement;
- Verify mbr's access in NCAMS, QIS, and consult with USS;
- Assist mbrs filling DND 4473 Section A & CSSF-020 Special Indoc Form Gamma;
- Sign and Send SCI Request to NSC for processing.

NSC

- Begins SCI Request Process.
- Liaise with DGDS (Security Clearance)
- Liaise with CSE (Subject Verification and Credit Check)
- Receives Security certificates from DGDS & CSE
- Issues Authority to Indoc to COMCO team.

COMCO

- COMCO Team Direct Member to complete SIGINT knowledge test
- COMCO Team Schedule Indoctrination appointment (In-person/MS Teams).
- Completed Signed Indoc package sent to NSC for Processing.
- NSC Sends Transmittal of Clearance DTG.

SSO

- Mbr obtains CAC and Purple Badges prior next steps.
- Mbr takes TOC DTG to SSO.
- SSO confirms receipt and mbr's access using TOC DTG through RMT.
- SSO issues Green Badge to mbr.

~6 to 8 months Process

CAN UNCLASSIFIED



CAN UNCLASSIFIED

SCIF Access Security Policy

- Prohibition on electronic and medical devices inside SCIF;
 - Personnel must consult US SSO to verify if their devices are on the approved list.
 - Mbr must request formal US SSO approval prior wearing device into Secured Workspaces.
- Escort duties and responsibilities for cleared and uncleared personnel.
 - VCRs/VARs must be submitted ahead of time (45-30 days) to CDLS(W) and NSC, Visitor Passes must be requested to the US SSO, Escort must provide Security Briefing before proceeding inside the secure area.
 - If Visitors are TS only or only have one of the required Compartmented access, then they must turn the red lights on and have the visitors signed the visitor log on entry and enter their time of departure on completion of the visit.

Failure to comply may cause a loss of local access and security access removal.




CAN UNCLASSIFIED

Electronic Medical Device Request

Form - DAF110

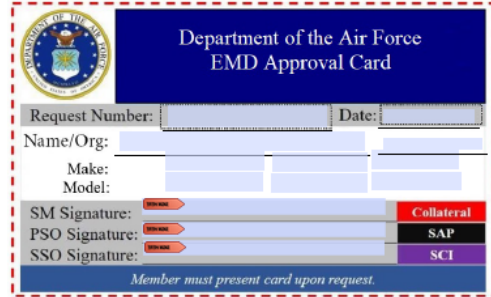
*Request Number (CMD-MM-YYYY-#):

CUI
(When Filled In)

Department of the Air Force (DAF) Electronic Medical Device (EMD) Request Form & Approval Card		
		
<small>Authority: Privacy Act of 1974, as amended and the "Defense Reasonable Accommodation and Assistive Technology Records" DoD 0007. Principal Purpose: The National Security Act of 1947, as amended. Routine Uses: Evaluation and approval for individuals are requested to utilize EMDs in DAF secure spaces. Disclosure: Only on an as-needed basis for purposes of implementing this request. Disclosure of information is voluntary; however, failure to provide requested information will prevent further processing.</small>		
1. REQUESTER INFORMATION		
Name (Last, First, MI):	Rank/Grade:	
Organization:	Phone:	
2. DEVICE INFORMATION		
Make:	Model:	Serial Number:
Make:	Model:	Serial Number:
Make:	Model:	Serial Number:
3. USER AGREEMENT		
By my signature below, I understand:		
a. My responsibilities and have been briefed on the requirements for utilization of this EMD within DAF secure spaces.		
b. That the U.S. Government (USG), through a designated representative of the Department of Defense (DoD), may seize my EMD for security purposes and that the USG or its designee may conduct a physical and forensic examination of the device. I understand that EMDs seized as evidence of a crime or security incident will be handled under DoD investigative policies. In some cases, EMDs may be permanently retained, destroyed, or have their data and operating systems wiped resulting in loss of information.		
c. Questions concerning loss or damage to a personally-owned EMD should be directed to the base or servicing legal office.		
d. That it remains my inherent responsibility to fully protect all sensitive material in my custody, ensuring against loss or compromise. Nothing in the foregoing shall be construed to excuse my use of good judgment and common sense to provide maximum security protection of the information entrusted to my possession.		
e. I am only allowed to bring in those devices approved by the Security Manager (or his/her representative), Program Security Officer, or Special Security Officer, as annotated on this form.		
f. That I must maintain the EMD approval card and present it upon request, within any DAF secure space.		
Signature:		(MM/DD/YYYY):
AUTHORIZATIONS		
4. COLLATERAL SECURE SPACE AUTHORIZATION		
SECURITY MANAGER OR DESIGNATED REPRESENTATIVE		
Name (First MI, Last):	Rank/Grade:	
Organization:	Email:	Duty Phone:
Signature:		Date (MM/DD/YYYY):
INFORMATION SYSTEM SECURITY MANAGER		
Name (First MI, Last):	Rank/Grade:	
Organization:	Email:	Duty Phone:
Signature:		Date (MM/DD/YYYY):
Note: If the requester operates out of a SAP or SCI secure space, skip section 4., and proceed to the next page.		

Controlled By: [Organization]

CUI
(When Filled In)

5. SPECIAL ACCESS PROGRAM SECURE SPACE AUTHORIZATION		
PROGRAM SECURITY OFFICER		
Name (First MI, Last):	Rank/Grade:	
Organization:	Email:	Duty Phone:
Signature:		Date (MM/DD/YYYY):
INFORMATION SYSTEM SECURITY MANAGER		
Name (First MI, Last):	Rank/Grade:	
Organization:	Email:	Duty Phone:
Signature:		Date (MM/DD/YYYY):
6. SENSITIVE COMPARTMENTED INFORMATION SECURE SPACE AUTHORIZATION		
SPECIAL SECURITY OFFICER		
Name (First MI, Last):	Rank/Grade:	
Organization:	Email:	Duty Phone:
Signature:		Date (MM/DD/YYYY):
INFORMATION SYSTEM SECURITY MANAGER		
Name (First MI, Last):	Rank/Grade:	
Organization:	Email:	Duty Phone:
Signature:		Date (MM/DD/YYYY):
EMD Card		
		
Provide copy of EMD Approval Card to Requester		

*Request Number Details: e.g. ACC-04-2023-5 (Air Combat Command-April-2023-5th Request of the Calendar Year)

CAN UNCLASSIFIED


PWFD Request

Form - DAF111

*Request Number (CMD-MM-YYYY-#):

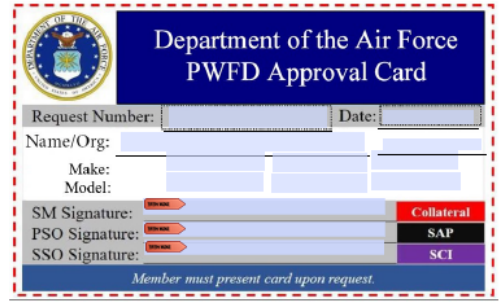
CUI

(When Filled In)

		Department of the Air Force (DAF) Personal Wearable Fitness Device (PWFD) Request Form & Approval Card	
<small>Authority: Privacy Act of 1974, as amended and the "Defense Reasonable Accommodation and Assistive Technology Records" DoD 9007. Principal Purpose: The National Security Act of 1947, as amended. Disclosure: Evolution and approval for individuals are requested to utilize EODs in DAF secure spaces. Only on an as-needed basis for purposes of implementing this request. Disclosure of information is voluntary; however, failure to provide requested information will prevent further processing.</small>			
1. REQUESTER INFORMATION			
Name (Last, First, MI):		Rank/Grade:	
Organization:		Phone:	
2. DEVICE INFORMATION			
Make:	Model:	Serial Number:	
Make:	Model:	Serial Number:	
Make:	Model:	Serial Number:	
3. USER AGREEMENT			
By my signature below, I understand:			
a. My responsibilities and have been briefed on the requirements for utilization of this PWFD within DAF secure spaces. b. That the U.S. Government (USG), through a designated representative of the Department of Defense (DoD), may seize my PWFD for security purposes and that the USG or its designee may conduct a physical and forensic examination of the device. I understand that PWFDs seized as evidence of a crime or security incident will be handled under DoD investigative policies. In some cases, PWFDs may be permanently retained, destroyed, or have their data and operating systems wiped resulting in loss of information. c. Questions concerning loss or damage to a personally-owned PWFD should be directed to the base or servicing legal office. d. That it remains my inherent responsibility to fully protect all sensitive material in my custody, ensuring against loss or compromise. Nothing in the foregoing shall be construed to excuse my use of good judgment and common sense to provide maximum security protection of the information entrusted to my possession. e. I am only allowed to bring in those devices approved by the Security Manager (or his/her representative), Program Security Officer, or Special Security Officer, as annotated on this form. f. That I must maintain the PWFD approval card and present it upon request, within any DAF secure space.			
Signature:		(MM/DD/YYYY):	
AUTHORIZATIONS			
4. COLLATERAL SECURE SPACE AUTHORIZATION			
SECURITY MANAGER OR DESIGNATED REPRESENTATIVE			
Name (First MI, Last):		Rank/Grade:	
Organization:		Duty Phone:	
Signature:		Date (MM/DD/YYYY):	
INFORMATION SYSTEM SECURITY MANAGER			
Name (First MI, Last):		Rank/Grade:	
Organization:		Duty Phone:	
Signature:		Date (MM/DD/YYYY):	
Note: If the requester operates out of a SAP or SCI secure space, skip section 4., and proceed to the next page.			

CUI

(When Filled In)

5. SPECIAL ACCESS PROGRAM SECURE SPACE AUTHORIZATION			
PROGRAM SECURITY OFFICER			
Name (First MI, Last):		Rank/Grade:	
Organization:		Duty Phone:	
Signature:		Date (MM/DD/YYYY):	
INFORMATION SYSTEM SECURITY MANAGER			
Name (First MI, Last):		Rank/Grade:	
Organization:		Duty Phone:	
Signature:		Date (MM/DD/YYYY):	
6. SENSITIVE COMPARTMENTED INFORMATION SECURE SPACE AUTHORIZATION			
SPECIAL SECURITY OFFICER			
Name (First MI, Last):		Rank/Grade:	
Organization:		Duty Phone:	
Signature:		Date (MM/DD/YYYY):	
INFORMATION SYSTEM SECURITY MANAGER			
Name (First MI, Last):		Rank/Grade:	
Organization:		Duty Phone:	
Signature:		Date (MM/DD/YYYY):	
<div style="text-align: center;"> PWFD Card </div> 			
Provide copy of PWFD Approval Card to Requester			

*Request Number Details: e.g. ACC-04-2023-5 (Air Combat Command-April-2023-5th Request of the Calendar Year)



CAN UNCLASSIFIED

PED User Agreement

USER AGREEMENT FOR PERSONALLY OWNED PORTABLE ELECTRONIC DEVICES

Name (Last, First, MI):

Grade:

SSN (Last 4):

Office:

Duty Phone:

Make:

Model:

S/N:

1. By my signature below, I acknowledge that:

a. I understand my responsibilities and will comply with procedures set forth in the NORAD and USNORTHCOM (N&NC) / Special Security Office (SSO), "Sensitive Compartmented Information Facility (SCIF) Portable Electronic Device (PED) Policy."

b. I understand that the U.S. Government (USG) through a designated representative of the Department of Defense (DoD) may seize my PED for security purposes and that the USG or its designee may conduct a physical and forensic examination of the PED. I understand that PEDs seized as evidence of a crime or security violation will be handled under DoD Investigative Policies. In some cases, PEDs may be permanently retained, destroyed, or have their data and operating systems wiped resulting in loss of information.

c. I understand that if I have a legitimate claim for loss or damage to a personal PED, not lost or damaged through my own negligence or violation of security procedures, that I may file a claim in accordance with claims procedures administrated by the military departments.

d. I am fully aware that it remains my inherent responsibility as a DoD Employee, or member of the armed forces assigned to DoD, to fully protect all sensitive material in my custody, ensuring against loss or compromise. Nothing in the foregoing shall be constructed to excuse my use of good judgment and common sense to provide maximum security protection of the information entrusted to my possession.

e. I understand that I am only allowed to bring devices approved by the SSO into N&NC SCIFs and not authorized to bring devices into any Compartmented Areas or SAPFs.

f. I understand that I must keep my PED Card on person and will present upon request.

Submit this form to the Physical Security OMB: n-np.peterson.n-npj2.mbx.sso-physical-security-omb@mail.mil

Member's Acknowledgment

(Printed Name)

(Signature or Digital Signature)

(Date)

SSO's Approval

(Printed Name)

(Signature or Digital Signature)

(Date)

PRIVACY ACT STATEMENT

Authority: The National Security Act of 1947, as amended authorize collection of this information.
Principle Purpose: The information is collected to provide Special Security Officers ability to manage employee use of PEDs.
Routine Use: The information is collected to provide Special Security Officers ability to manage employee use of PEDs.
In addition to these disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the Department of Defense as a routine use pursuant to 5 U.S.C. 552a(d)(5) as follows:
The DoD "Blanket Routine Uses" set forth at the beginning of N&NC's compilation of systems of records notices apply to this system.
Disclosure: This information is requested on a voluntary basis. However, not providing the information could have an impact on determining PED use eligibility.

NORAD & USNORTHCOM	
PED CARD	
Name:	
Duty Phone:	
Make:	
Model:	
SN:	
SSO Signature:	
<i>Member must present card upon request.</i>	

CAN UNCLASSIFIED



CAN UNCLASSIFIED

SCI Inductee's Responsibilities

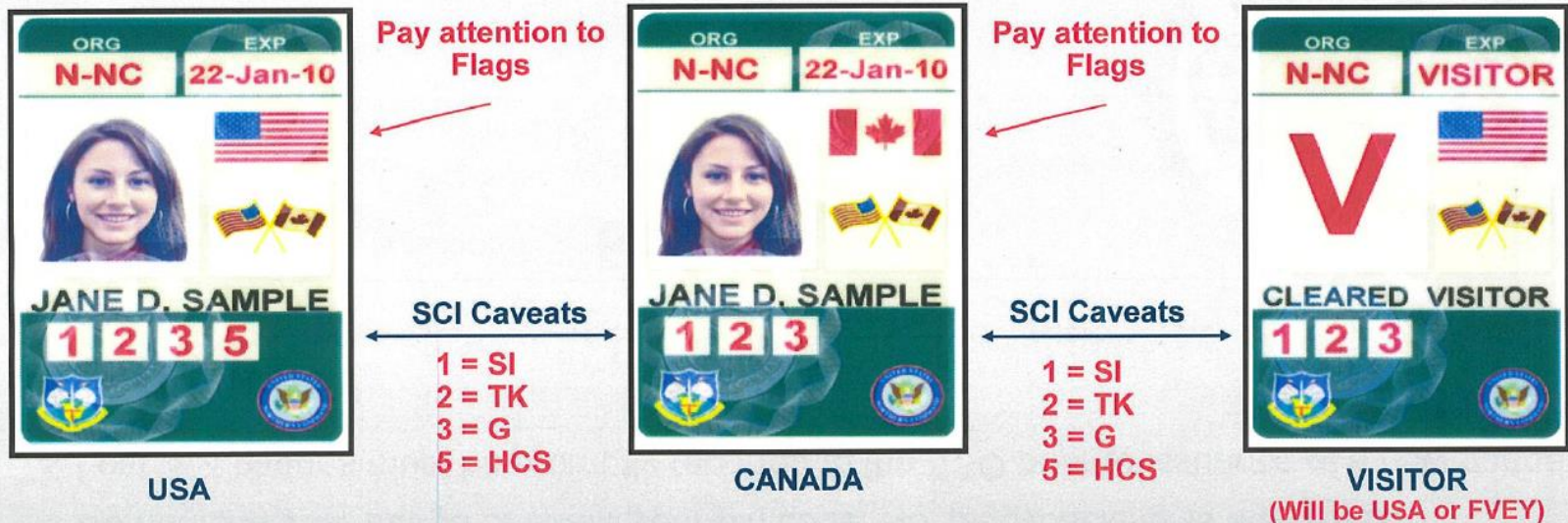
- Comply with SCI Security Standards and Policy:
 - Protect & Safeguard SCI material;
 - Maintain Security clearance up-to-date;
 - Confirm “Need-to-know” prior discussing/sharing;
 - Always protect your access card(s);
 - Do not bring unauthorized devices into a SCIF;
 - Report any Change of Circumstances;
 - Report any foreign contact or interference;
- Report all SCI related security incidents;
- Do not use access inappropriately;
- Continue to protect SCI material after De-indoctrination

CAN UNCLASSIFIED

Verifying Access

UNCLASSIFIED//FOUO

SCIF BADGES



All personnel must have a green SCIF badge to enter a SCIF

SCIF badges are for DISPLAY ONLY

UNCLASSIFIED//FOUO

Contact Us



**For All COMCO and SCI inquiries, DO NOT contact individuals on the team,
DO contact the general ++ mailbox at:**

CANELEMNORADCOMCO-OCICCANELEMNORAD@forces.gc.ca

**++CANELEMNORAD COMCO – OCIC CANELEMNORAD@CANELEMNORAD
DCOMD NORAD@COLORADO SPRINGS, US**

For getting a hold of the US COMCO-equivalent or SSO:

N-NC SSO (Special Security Office)

Tel: 719-554-5761 / 719-554-0936

NIPR: (1) n-nc.Peterson.n-ncj2.mbx.j2sso-persec-omb@mail.mil

(2) n-nc.Peterson.n-ncj2.mbx.sso-physical-security-omb@mail.mil

TS(JWICS): norad-northcomsso@coe.ic.gov

SharePoint (NIPR): [https://dod365.sharepoint-mil.us/sites/NORAD-USNC-
Command-Security](https://dod365.sharepoint-mil.us/sites/NORAD-USNC-Command-Security)



CAN UNCLASSIFIED

COMCO

Questions ?

CAN UNCLASSIFIED