DON CIO Telework Reference Guide

Ref: (a) Acceptable Use of Department of Navy Information Technology of 25 FEB 20
(b) Department of the Navy Telework Policy of 11 FEB 19

This reference guide highlights Information Technology (IT) resources and tools available to support telework. Per reference (a), all DON users must adhere to the DON IT acceptable policy.

Per reference (b), supervisors are responsible for ensuring employees are (1) in a position authorized for telework, (2) completed the required training, and (3) have a signed telework agreement (DD Form 2946) on file. In addition, each employee is required to complete a System Authorization Access Request (SAAR) and satisfy the mandated annual DoD Information Awareness and Personable Identifiable Information (PII) training requirements.

Employees are required to have an approved Property Pass (OF-7) when transporting government equipment in and out of government facilities. Download a Property Pass here: OF-7

*To access links in this document, right-click, and choose "Copy Hyperlink," then paste in web browser.

1. Actions Required Prior to Commencement of Telework

All users should run a Green Shutdown at COB each day and take their NMCI laptops home each evening. Ensure you have a CAT 5 cable to connect your laptop directly to your home router. NMCI H: Drive users should copy active H: Drive files to their Desktop to access offline.

Users planning to connect via personal IT equipment, ensure you have a DoD approved external CAC reader and a computer running WIN10 if available. Detailed instructions for Apple users.

Employees should verify the expiration of your DoD CAC and renew if expiring in the next 30 days.

Employees are also encouraged to logon to MILCONNECT to update email, command info, and new contact information to update the NMCI GAL: https://milconnect.dmdc.osd.mil/milconnect

A NMCI PIN will be required to request assistance from NMCI while working remotely. To establish an NMCI PIN, please go to: https://servman/sm/ess.do Navigate from the left-hand panel to: Authentication Information. Click on your name to establish or update your NMCI PIN.

2. Network Connection Options (OWA, VPN, MobiKEY, BlackBerry Work)

Outlook Web Access (OWA). OWA is a Common Access Card (CAC)-enabled, web-based email client with the look and feel of the Outlook client and is the preferred method to connect to the network while working remotely. OWA allows users access to their mailboxes and calendars from any Internet connection regardless of whether or not the computer is equipped with Outlook. It is recommended to connect your NMCI laptop directly to your home router, using a CAT 5 cable. Detailed instructions to access OWA are available at: Outlook Web Access (OWA) SOP

- Navy East Coast users can access OWA at: https://webmail.east.nmci.navy.mil
- NMCI Office 365 pilot users can access OWA at: https://webmail.cloud.navy.mil
- MCEN Office 365 pilot users can access OWA at: https://O365.usmc.mil

Virtual Private Network (VPN). Pulse Secure VPN software provides remote and mobile users with secure, authenticated access to Navy Marine Corps Intranet (NMCI) Non-secure Internet Protocol Router Network (NIPRNet) e-mail services, shared drives, and DoD CAC enabled websites. Detailed instructions for use of the Pulse Secure VPN software are available at: Virtual Private Network (VPN) SOP

- While a number of remote access options are available, the network capacity to deliver full VPN access from remote locations is limited. Exceeding this capacity in a mass telework scenario could compromise mission requirements by preventing some personnel from accessing the network entirely, or limiting functionality and performance levels. Given this scenario, VPN connectivity will be limited to those users who have an operational requirement to utilize full remote desk-top level functionality.

MobiKEY. MobiKEY allows users to securely view and control the NMCI host computer and applications, providing access to NMCI services as if the user were at the office. All files stay on the NMCI host computer securely within the defense enclave. For employees issued a MobiKEY, detailed instructions for use of MobiKEY are available at: MobiKEY SOP

BlackBerry Work. Government issued iPhones with BlackBerry (BB) Work. BB Work allows users to access NMCI NIPRNet email, Calendar, and Contacts. Current iPhone users should use the Blackberry Work App on their government issued device to access NMCI resources. For employees issued a government phone, detailed instructions for use of BB Work are available at: BlackBerry Work SOP

3. Collaboration Tools (DCS, Pentagon Conference Bridge)

Defense Collaboration Services (DCS). DCS provides secure web conferencing and instant messaging on the NIPRNet, and is accessible via the Internet. DCS resides on MilCloud, a virtualized datacenter hosting environment, and supports CAC and select hard token holders and guest (DoD mission partners) users. Detailed instructions for use of DCS are available at: Defense Collaboration Services (DCS)

Pentagon Conference Bridge. Your Joint Service Provider (JSP) VoIP desk Phone can be configured to host conference calls. These Pentagon conference bridges can handle up to 30 callers. Detailed instructions for setup and operation are available at: Pentagon Conference Bridge SOP

4. Large File Transfer Tools

DoD Safe

https://safe.apps.mil

DoD SAFE (Secure Access File Exchange) is a service to make it easy for you to exchange unclassified files up to 8.0 GB that can't be sent through email.

Please note: Non-DoD Personal Identity Verification (PIV) certificates or External Certificate Authority (ECA) are not currently supported. Users should select their SIGNATURE certificate issued through the

DoD email Certificate Authority (CA) or select the AUTHENTICATION PIV certificate issued by the DOD Identifier (ID) Certificate Authority (CA) in order to connect. Users outside of DoD may notice lengthy download and upload times depending on their bandwidth availability, but DISA will work to continually improve the experience for all users.

Intelink ISAFE
https://isafe.intelink.gov

ISAFE allows users to transfer files to higher classification networks

You are currently on the Unclass network. Destination networks are SIPR and JWICS. You must register for an account on intelink to access this tool.

5. Help Desk Support

For NMCI users, contact the NMCI Service Desk at ***1-866-843-6624*** for assistance.

For MCEN users, contract the USMC Enterprise Service Desk at ***1-855-373-8762*** for assistance.

- Detailed U.S Marine Corps Enterprise Network Remote Access Preparedness Planning Guidance is available at: USMC Remote Access Guidance

SECNAV Staff users can also contact the DON CIO IT Help Desk at ***1-703-695-6009*** for assistance.