UNCLASSIFIED//

ROUTINE

R 172159Z MAR 20 MID110000481380U

FM CNO WASHINGTON DC

TO NAVADMIN

INFO CNO WASHINGTON DC

BT
UNCLAS
PASS TO OFFICE CODES:
FM CNO WASHINGTON DC/N2N6//
INFO CNO WASHINGTON DC/N2N6//

MSGID/GENADMIN/CNO WASHINGTON DC/N2N6/MAR//

NAVADMIN 068/20

SUBJ/EFFECTIVE USE OF REMOTE WORK OPTIONS//

REF/A/NAVADMIN/OPNAV/122210ZMAR20//

REF/B/NAVADMIN/OPNAV/142000ZMAR20//

REF/C/ALNAV/SECNAV/121914ZMAR20//

REF/D/MEMO/DON CIO/ACCEPTABLE USE OF DEPARTMENT OF THE NAVY INFORMATION TECHNOLOGY/25FEB2020//

REF/E/WEBPAGE/RAS GUIDE FOR NMCI USERS//

NARR/REF A IS NAVADMIN 064/20, NAVY MITIGATION MEASURES IN RESPONSE TO CORONAVIRUS OUTBREAK.
REF B IS NAVADMIN 065/20, NAVY MITIGATION MEASURES IN RESPONSE TO CORONAVIRUS OUTBREAK UPDATE 1.
REF C IS ALNAV 025/20, VECTOR 15 FORCE HEALTH PROTECTION GUIDANCE FOR THE DEPARTMENT OF THE NAVY (DON).
REF D IS DON CIO ACCEPTABLE USE OF DEPARTMENT OF THE NAVY INFORMATION TECHNOLOGY.
REF E IS REMOTE ACCESS SERVICES WEBSITE FOR NMCI USERS AT https ://homeport.navy.mil/support/topics/remote-access-services-(ras)/?sort=date&page=1.//

POC/ERIC MCCARTNEY/CAPT/OPNAV N2N6G32/EMAIL: ERIC.S.MCCARTNEY(AT)NAVY.MIL /TEL: 571-256-8399/DSN 312-260-8399//

RMKS/1. This is a joint OPNAV N2N6 and Fleet Cyber Command, and Commander TENTH Fleet message.

2. In addition to references (a) and (b), and to further mitigate the spread of Coronavirus Disease 2019 (COVID-19), reference (c) directed implementation of maximum telework flexibilities for shore commands, consistent with command operational needs as determined by their heads.

3. The Joint Force Headquarters for Department of Defense Information Networks (JFHQ-DODIN) has begun to initiate the blocking of streaming media websites (YouTube, Netflix, Pandora, etc.) and may soon block social media websites (Facebook, Instagram, etc.) to maximize operational bandwidth available for COVID-19 response. Exceptions to these policies with mission justification may be approved by O6/GS-15 or above and submitted via Fleet Cyber Command Battle Watch Captain at EMAIL: c10f_bwc.fct(at)navy.mil.

4. The following guidance applies to shore commands using Navy and Marine Corps Intranet (NMCI) and ONE-NET, describing the capacity of remote work resources and the priority in which they should be leveraged. We must be prudent and optimize the utilization of the available network resources. Currently, NMCI and ONE-NET can support roughly 240,000 simultaneous connections for Outlook Web Access (OWA) and 40,000 for Virtual Private Network (VPN) access. NAVWAR and PMW-205 are working to expand capacity, where possible, over the next several weeks. There are a limited number of Mobikey and Enhanced Virtual Desktop (EVD)/Virtual Desktop Infrastructure (VDI) instances that may be used to support telework. Navy does not intend to negotiate any more licenses. Navy has issued 35,000 Blackberry Unified Endpoint Management (UEM) devices (iPhone, iPad and other mobile devices). Bandwidth limitations preclude the addition of new devices.

5. Utilize remote work options in the following prioritized order:

a. Mobikey and EVD.

b. Mobile devices with Blackberry UEM. Consider downloading all of the Blackberry Work / Edit / Access applications to get full capability, including the ability to edit documents. Reach to your local support team for help in getting these apps on your phone.

c. OWA. Ensure OWA users have a signed agreement and are well trained on OWA requirements and best practices. Command Access Card (CAC) readers are required for use with OWA. A CAC reader that has been used on a personal computer may NOT be brought back to work and used to connect to the DOD Information Networks (DoDIN). If a government CAC reader is brought home and used, it must remain at home. Individual commands will determine whether individuals should bring Government CAC readers home permanently to support OWA use. As heavy OWA use is expected during the implementation of these measures, users should connect periodically to stay updated, but disconnect afterward to facilitate access for other remote users. Users with government laptops should access email via OWA vice Remote Access Service (RAS) whenever possible to reduce RAS connection load. Naval Network Warfare Command (NETWARCOM) enabled OWA to support file download and upload when using Internet Explorer (IE) ONLY. Other browsers will not permit download or upload of attachments as files. The use of IE for file download and upload provides new, additional flexibility while using OWA and should relieve some of the need for RAS access.

d. RAS. Use in accordance with references (d) and (e). The ratio of government laptops to available connections is about four to one (159,000 devices with only 40,000 simultaneous connections available). Again, personnel with government laptops should connect via OWA for email access as a first option to limit RAS connection load. Using RAS when needed; personnel should only connect to download or transmit emails, or to access other resources only accessible by VPN, and then log off to reduce RAS connection load. Work offline until next period needed to transmit/receive/access. NETWARCOM is implementing time restrictions on the VPN, so expect to be kicked off if you are logged on too long.

6. Defense Collaboration Services (DCS) is an available option for collaboration and virtual meetings at https://conference.apps.mil. SharePoint portals may be used for collaboration and file sharing, including Milsuite at https://www.milsuite.mil. Navy users should use only the DoD approved collaboration tools and not seek out commercial collaboration sources for DoD-only events.

7. Mobile SIPRNET Device. Senior leaders requiring mobile SIPRNET access may submit a request for a DoD Mobility Classified Capabilities (DMCC) device via echelon II Command Information Officer (CIO). Due to limited number of devices, echelon II CIO requests will be consolidated and reviewed by OPNAV N2N6 for submission to Defense Information Systems Agency (DISA).

8. Additional remote work guidance:

a. Properly protect ALL Personally Identifiable Information (PII) and Protected Health Information (PHI) data.

b. One significant limitation of OWA use is inability to encrypt or decrypt emails by default. One alternative is to enable encryption via OWA by user intervention (by making the OWA link a Trusted Site in browser security settings and enabling S/MIME control). See the instructions posted on the references page listed in paragraph 11. Another alternative is the use of Department of Defense (DoD) Secure Access File Exchange (SAFE) as described below in paragraph 8.

c. If you need to purchase your own CAC reader, https://milcac.us/tweaks lists the types of CAC readers best for your personal computer operating system.

d. For OWA, a government laptop should be the first choice; if no government laptop is assigned, use of a personal computer is permitted ONLY if a proper antivirus solution such as Microsoft Defender is operating on the device. Antivirus solutions must be kept up to date.

e. Limit attachment file size to minimize network impact and prevent hitting inbox size limits. If you must send large files, use services like DoD SAFE (https://safe.apps.mil).

f. Limit use of REPLY TO ALL when responding to group emails to minimize network traffic.

g. SIPRNET and JWICS accounts will continue to be disabled after 30 days without activity. Consider logging in periodically to keep classified accounts active, even during this period of maximizing remote work.

9. For secure and/or large file transfers, DoD SAFE is available for use. Both DoD CAC users and guests can use the service for UNCLASSIFIED files up to 8GB in size. DoD SAFE is approved for transfer of FOR OFFICAL USE ONLY (FOUO), PII, and PHI data. More information and the link to DoD SAFE can be found at the following link:
https://www.doncio.navy.mil/ContentView.aspx?id=12723

10. When using remote work options, information security is paramount. As we continue to operate in remote work environment, we cannot allow ourselves to violate security protocols. Using personal e-mail and other commercial services (e.g.: Gmail, Zoom, WebEx, and others) for official business is not permitted. The potential vulnerabilities open the door for our adversaries to collect information that could be used against us. Getting the job done at the expense of information security is unacceptable. It is better that work be delayed than be done in a way that compromises information.

11. The NMCI and ONE-NET Help Desks are still the best avenue for help for individual users, along with seeking support with local representatives, such

as NMCI assistant contract technical representatives (ACTRs).

12. References in this NAVADMIN and links to additional remote work guidance can be found at https://portal.secnav.navy.mil/orgs/OPNAV/N2N6/DDCION/N2N6BC1/SitePages/Effective%20Use%20of%20Remote%20Work%20Options.aspx

13. Request widest dissemination. This NAVADMIN will remain in effect until cancelled or superseded.

14. Released by VADM Matthew J. Kohler, Deputy Chief of Naval Operations for Information Warfare, OPNAV N2N6.//

BT
#0001
NNNN
UNCLASSIFIED//