DEPARTMENT OF THE NAVY
COMMANDER NAVY RESERVE FORCE
1915 FORRESTAL DRIVE
NORFOLK, VIRGINIA 23551-4615

COMNAVRESFORINST 1000.9A
N5
1 Jul 15

COMNAVRESFOR INSTRUCTION 1000.9A

From: Commander, Navy Reserve Force

Subj: TELEWORK POLICY FOR NAVY RESERVE SERVICE MEMBERS

Ref: (a) DoD Instruction 1035.01 of 4 April 2012
(b) SECNAVINST 12271.1
(c) RESPERS M-1001.5, Navy Reserve Personnel Manual
(d) Joint Travel Regulations

Encl: (1) Administrative Remarks NAVPERS 1070/613 (Sample)
(2) COMNAVRESFOR Telework Information Technology Strategy

1. Purpose. To establish policy and identify telework program requirements for service members of the Navy Reserve.

2. Cancellation. COMNAVRESFORINST 1000.9.

3. Background. The Telework Enhancement Act of December 2010 emphasizes the strategic value that federal agencies receive from telework. This program is designed to promote telework as a valued method for Navy Reserve service members to meet mission requirements. Telework is the practice of performing assigned military duties at the service member's home of record and/or within the local area of their home. Travel reimbursement and/or per diem is not authorized. It is a management option meant to increase flexibility and productivity while maximizing resources—not to be used for the convenience of the member and/or a substitute for dependent care.

4. Scope. This instruction applies to all Ready Reserve Service Members (Full-time Support (FTS), Selected Reserve, Voluntary Training Unit and Active Status Pool).

a. FTS and Reserve members on Active Duty for Special Work (ADSW) shall follow procedures established by this instruction, references (a) through (d) and all applicable supported command directives. Anticipate the future inclusion of Annual Training/Active Duty for Training telework to this instruction upon completion of a Navy Reserve Order Writer System (NROWS) program build required for telework tracking and auditing.

b. Personnel requesting to telework while in a drill status shall follow procedures established by this instruction and references (a) through (c). When authorized, telework may be used for pay and non-pay drills, but credit shall not be given for conducting physical fitness.

5. Policy. It is Commander, Navy Reserve Force (CNRF) policy that:

a. Telework training will be accomplished prior to requesting and/or acting in a supervisory role for counseling a potential telework applicant.

b. Prior to commencing telework, the following forms shall be completed, signed, approved, and routed for proper filing:

(1) Commander, Navy Reserve Force Telework Eligibility Checklist (NAVRES 1000/7).

(2) Commander, Navy Reserve Force Telework Request Form (NAVRES 1000/8).

(3) Department of Defense Telework Agreement (DD Form 2946, DEC 2011).

(a) This form shall be reviewed and re-validated annually.

(b) If any conditions and/or locations change, this form shall be completed in its entirety and the entire telework package resubmitted for approval.

(4) Administrative Remarks (NAVPERS 1070/613) form to acknowledge member's accountability and personal responsibility to include coverage by the Uniform Code of Military Justice and other pertinent regulations concerning determination for line of duty, injury/illness and misconduct. A sample is provided in enclosure (1).

c. Participants shall meet all administrative, medical, and training readiness requirements.

d. Eligibility is discretionary and determination shall be consistent with this instruction and references (a) and (c).

e. Participants shall not telework while simultaneously working a civilian job.

f. Participants shall adhere to the strategies delineated in enclosure (2) and current Information Technology (IT) policies. Performance of duties shall only involve dealing with unclassified materials.

6. Responsibilities

a. CNRF Inspector General (N002) and Echelon IV Commanders shall implement a mission applicable telework section for their inspection criteria for assessments of all commands under their cognizance.

b. The Commanding Officer (CO) or Officer-in-Charge (OIC) of a commissioned or non-commissioned unit shall:

(1) Determine if a telework program is appropriate for their command.

(2) If determined appropriate:

(a) Develop, implement, and ensure the command's telework program is consistent with this instruction and references (a) through (d).

(b) Be the approving authority for all requests. Retain records to meet Financial Improvement and Audit Readiness (FIAR) requirements.

(c) Ensure the command's telework program and participants are meeting mission requirements and maintaining individual readiness.

(3) Designate a Command Telework Program Coordinator (CTPC) if required.

c. CTPC shall:

(1) Maintain approved telework packages to include: copies of training completion certificates for both participants and supervisors, Telework Eligibility, Approval and Agreement forms, and a properly signed NAVPERS 1070/613.

(2) Ensure that approved telework packages receive an annual review and re-approval.

d. Supervisors shall:

(1) Be familiar with this instruction, references (a) through (d), supported command directives and how it applies to their command's telework program and applicants.

(2) Complete the required "Telework Training for Department of the Navy (DON) Supervisors," currently found on the DON Civilian Human Resources website and ensure a copy of the completion certificate is included in all applicants' telework packages.

(3) Make position eligibility determinations and assess applicants' eligibility for telework.

(4) Recommend telework approval/disapproval.

(5) Monitor the command's telework program to confirm it is meeting mission requirements and all participants are maintaining unit and individual readiness standards.

e. Service Members desiring to telework shall:

(1) Be familiar with and if approved, adhere to this instruction, references (a) through (d) and supported command directives.

(2) Complete the required "Telework Training for DON Employees," currently found on the Total Workforce Management System (TWMS)and include a copy of their completion certificate in their telework package.

(3) Submit the required forms for telework eligibility (NAVRES 1000/7) and request (NAVRES 1000/8) for approval.

(4) If approved, sign NAVPERS 1070/613 and include it along with a completed DD Form 2946 in the telework package for appropriate routing.

7. Forms. The following forms are available for download on the Navy Reserve Homeport and Naval Forms Website:

a. Commander, Navy Reserve Force Telework Eligibility Checklist, NAVRES 1000/7, (12-13).

b. Commander, Navy Reserve Force Telework Request Form, NAVRES 1000/8, (12-13).

c. Department of Defense Telework Agreement, DD Form 2946, Dec 2011.

R. R. BRAUN

Distribution:
Electronic copy via CNRF Web site
http://navyreserve.navy.mil.

ADMINISTRATIVE REMARKS
NAVPERS 1070/613 (REV. 08-2012) **PREVIOUS EDITIONS ARE OBSOLETE** **SUPPORTING DIRECTIVE MILPERSMAN 1070-320**

SHIP OR STATION:

SUBJECT: TELEWORK FOR SERVICE MEMBERS	□ PERMANENT ☒ TEMPORARY AUTHORITY *(IF PERMANENT)*:

(Date) : I, (Name) acknowledge my accountability and personal responsibility in the performance of duties while teleworking. This includes following the telework guidance in COMNAVRESFORINST 1000.9 and corresponding references. I furthermore acknowledge that while in any duty status I am subject to the Uniform Code of Military Justice and other pertinent regulations concerning determination for line of duty, injury and illness and misconduct.

____
Signature
Name/Date

____
Witness Signature
Name/Date

ENTERED AND VERIFIED IN ELECTRONIC SERVICE RECORD:

VERIFYING OFFICIAL RANK OR GRADE/TITLE:	DATE:	SIGNATURE OF VERIFYING OFFICIAL:	
NAME (LAST, FIRST, MIDDLE):		SOCIAL SECURITY NUMBER:	BRANCH AND CLASS:

FOR OFFICIAL USE ONLY
PRIVACY SENSITIVE

COMNAVRESFOR Telework Information Technology (IT) Strategy

This enclosure provides additional information on the IT capabilities available to support the telework policy.

1. The ability to conduct business in remote environments is critical to executing the mission of the Department of the Navy (DON). To maximize and protect this ability, users are reminded of their responsibility to practice good IT stewardship through responsible and effective use of DON IT resources.

2. Telework employees are responsible to protect all government information, including information defined as For Official Use Only (FOUO), Controlled Unclassified Information (CUI) and Personally Identifiable Information (PII). If handling this type of information outside of the workplace, criteria for the proper encryption and safeguarding of such information and data must be consistent with DON Information Assurance (IA) Policy. Specifically:

a. Teleworking employees who access FOUO, CUI or PII may only do so on encrypted government furnished equipment (GFE) or a government-provided solution such as MobiKEY, the Navy Reserve Homeport (NRH) private portal, Hosted Virtual Desktop (HVD), or other secure means requiring Common Access Card (CAC) access or two-factor authentication for access.

b. Extraction of FOUO, CUI, or PII from DON systems onto personal devices used for teleworking is prohibited.

c. The use of personal commercial email accounts for FOUO, CUI, or PII transmission is strictly prohibited. Email sent containing FOUO, CUI, or PII data may only be emailed between Government email accounts and must be encrypted and digitally signed by the sender. Additionally, it must be sent only to recipients with an official "need to know." Any breach of this policy must be reported to the Commander, Navy Reserve Forces Command (CNRFC) Information Assurance Manager (IAM).

3. Classified documents (hard copy or electronic) shall not be taken to or created at an employee's alternative worksite.

4. Prior to authorizing telework, supervisors will ensure telework employees have an approved System Authorization Access request on file. Additionally, all users shall complete and

stay current with their annual required Department of Defense (DoD) IA and PII training as a strict condition of continued access to the network. Both training courses are available online at www.nko.navy.mil.

5. If the telework employee uses GFE, the employee will use and protect the equipment at all times. GFE will be serviced and maintained by CNRFC. If the telework employee intends to use personal equipment, the employee agrees to comply with the terms of computer software license and copyright agreements and computer virus and protection requirements and procedures. Specifically, the employee is responsible to install the most current anti-virus software on his or her personal device and maintain an active software firewall.

6. GFE

a. CNRF encourages the use of GFE or HVD because it guarantees the segregation of government information from personal devices and adds the assurance of a defense-in-depth approach that includes device management controls, software releases and up to date anti-virus protection that may not be afforded with the use of personally owned equipment.

b. Use of GFE or HVD affords the opportunity of immediate action in the event unauthorized information has been processed and/or transmitted on the equipment via sanitization of the hard drive due to unauthorized use of CUI, such as PII or classified information, resulting in an electronic spillage.

7. Personally-owned Equipment

a. Use of personally-owned equipment, such as a personal computer, for telework is authorized when GFE is not provided or available. Hardware interface solutions such as MobiKEY may be available for use.

b. The use of personally-owned equipment for official business introduces a number of issues that could have negative impacts on both the government and the employee. Unlike GFE, personal devices cannot be integrated into the network's device management tools. Also, the government cannot ensure that the optimal anti-virus and other software tools are installed on personal devices. This is a personal responsibility.

8. Mixing government and personal data on one device is strongly discouraged. Storing any form of CUI, including PII,

is prohibited on personally owned computers, mobile computing devices and non-GFE removable storage media. Processing or storing classified information on personal IT equipment is strictly prohibited and disciplinary action will be taken.

9. If there is an unauthorized disclosure of classified or CUI information on a personal device, the government may have the right to confiscate the device and dispose of it as per current guidance on handling an electronic spillage, including the physical destruction of the hard drive. Potential classified information spillages or PII breaches must be reported immediately to CNRFC IAM (N64).

10. Telework employees utilizing personal devices will make every effort to collaborate and work on documents resident within NRH private portal. This eliminates the need to store government data on personal devices.

11. Remote Access Capability. CNRFC offers the following options for remote access.

a. Navy Marine Corps Intranet (NMCI) laptop.

b. HVD: HVD is a thin client desktop solution that provides access to all NMCI services. It also provides a secure Virtual Private Network (VPN) connection from remote locations via a web browser. This is the preferred hardware solution, if the member does not have an NMCI laptop.

c. A smart card reader: an external CAC reader that connects to a personally owned computer via a Universal Serial Bus (USB) port in order to support CAC login and authentication required for Outlook Web Access (OWA) and many official DoD sites.

d. MobiKEY: an external, CAC enabled, hardware device that remotely connects to a GFE system to enable full desktop capability.

12. Connection Options. Various options exist for connecting remote devices to the network. Many devices may be capable of network connectivity through two or more of these options. If their primary means of connecting fails, telework employees should try to connect with the next alternative in line.

a. Utilize your home internet access. This refers to using an internet site or portal to connect to the government network through any wired or wireless means. Teleworkers can access most unclassified DoD and DON CAC enabled web sites through the internet, however some government sites may only be accessed from a workstation on a ".mil" domain.

b. Access e-mail via OWA. This is one of the primary telework uses for web access, which provides a version of the desktop e-mail, e-mail contacts and calendar applications. While some functionality is lost with OWA, including access to network drives and other peripherals, remote access with OWA is practically unlimited for the network, may be used on personally-owned equipment if GFE is not available, is cost effective, may be used in conjunction with web portals and is the preferred telework solution for personnel whose remote work can be accomplished without network based services. The user should be aware that downloading documents from OWA for work may violate portions of these guidelines if the document contains PII.

c. Virtual Private Network (VPN). Provides a secure, encrypted connection onto a network from an outside location, through the use of a laptop or other devices. A VPN connected laptop can provide the same full range of network functionality as a desktop office computer. VPN access can be accomplished through a wired connection, a cellular air card or an approved Wireless Fidelity (Wi-Fi) connection. DON VPNs are based on either Internet Protocol Security (IPSEC) or Secure Sockets Layer (SSL). These are referred to respectively as an IPSEC VPN or SSL VPN. The SSL VPN is preferred when available, IPSEC is acceptable and both may be available on any given device. The number of VPN ports on the DON network is physically limited. Telework employees without a bona fide need for VPN functionality to meet their job requirements should utilize OWA.

d. Wireless Fidelity (Wi-Fi). Wi-Fi may include portable devices such as laptops, smartphones and tablets, which come with built in Wi-Fi capability, requires the issuance of an NMCI Wi-Fi card and associated software. Due to concerns over potential security exposures, use of Wi-Fi is strictly limited to:

(1) When in a public Wi-Fi "hot spot," offering such as coffee shops, airports or other public places, the only accepted method of connecting to a DON network via a public "hot spot" is a GFE laptop with the proper Designated Accrediting Authority

approved Wi-Fi solution, hardware and software. The use of a device's native Wi-Fi capability is not authorized.

(2) With the exception of access to OWA, as per the OWA User Responsibilities and Acknowledgement, residential home Wi-Fi network are allowed when set up in accordance with the current guidance from the DON Chief Information Officer and the National Security Agency.

(3) Cellular/Mobile Networks, such as DON BlackBerrys and other approved GFE smart phones and tablets, generally connect through a commercial cellular network as their primary link to the network. Some BlackBerrys support tethering, connecting a laptop to the device for Internet access instead of using an air card, which should be utilized, when available, due to the significantly reduced cost.