COMNAVRESFOR INSTRUCTION 12610.2A

From: Commander, Navy Reserve Force

Subj: TELEWORK POLICY FOR CIVILIAN EMPLOYEES

Ref: (a) DoD Instruction 1035.01 of 4 April 2012
     (b) SECNAVINST 5239.3B

Encl: (1) COMNAVRESFOR Telework Information Technology Strategy

1. Purpose. This instruction establishes policy and identifies requirements for the Commander, Navy Reserve Force (COMNAVRESFOR) civilian telework program. COMNAVRESFOR supports the telework concept in compliance with guidance outlined in references (a) and (b). This instruction is a complete revision and should be reviewed in its entirety.

2. Cancellation. COMNAVRESFORINST 12610.2.

3. Discussion. This program is designed to actively promote telework as a valued method to meet mission requirements for federal civilian employees throughout the Navy Reserve Force. The objectives of this program are to:

   a. Promote the Department of Navy (DON) and COMNAVRESFOR as an employer of choice.

   b. Improve the retention and recruitment of high-quality employees.

   c. Enhance COMNAVRESFOR's ability to provide an accommodation to qualified individuals with a disability to enable the employee to perform the essential functions of a job or enjoy the equal benefits and privileges of employment that are enjoyed by other similarly situated employees without disabilities.

   d. Reduce traffic congestion.

   e. Decrease energy consumption and pollution emissions.
f. Reduce office space, parking facilities and transportation costs, including costs associated with payment of the transit subsidy.

4. **Applicability.**

   a. This policy applies to all Federal civilian employees of COMNAVRESFOR and subordinate organizations.

   b. Prior to implementing a telework program for civilian positions in exclusively recognized bargaining units, commands/activities must satisfy bargaining obligations.

5. **Policy.** It is COMNAVRESFOR policy that:

   a. Prior to commencing telework, eligible employees shall complete the Commander, Navy Reserve Force Telework Eligibility Checklist (NAVRES 1000/7), Commander, Navy Reserve Force Telework Request Form (NAVRES 1000/8), Department of Defense (DoD) Telework Agreement (DD Form 2946, DEC 2011) and required telework training. All employees approved for telework shall adhere to the Information Technology (IT) policy in enclosure (1).

   b. Employees desiring to telework shall follow procedures established by reference (a), this instruction and their respective command’s telework policy.

   c. Performance of duties will involve only unclassified issues and material.

   d. During either natural or manmade emergencies, civilian employees who perform mission-critical duties may be required to work from home, at an alternate workplace or from their regularly designated workplace. This is an effort to ensure continuity of operations and employees should have a telework agreement on file. Employees with approved regular or situational telework agreements in place are expected to telework for the duration of any emergency and pursuant to:

      (1) A pandemic health crisis.

      (2) When the regular worksite is closed or closed to the public due to natural or manmade emergency situations.

      (3) When government offices are open with the option for unscheduled telework. This would typically occur when weather conditions make commuting hazardous or circumstances
arise that compromise employee safety (e.g., snowstorm, hurricane, act of terrorism, etc.).

e. Supervisors must ensure employees with approved regular or situational telework agreements have an appropriate amount of work to complete during the workday at home, should emergency situations (i.e., base closed due to unsafe weather conditions) arise. If an employee does not have enough work on that day, he or she must either take unscheduled leave for the entire workday or use a combination of unscheduled leave and unscheduled Telework to account for hours they do not work. Supervisors may also approve employees' request for use of appropriate leave during a period of unscheduled Telework.

6. Responsibilities

a. COMNAVRESFOR will:

(1) Promote the use of the Civilian Telework Program when such use does not adversely impact mission requirements.

(2) Comply with statutes, regulations, guidance and directives from higher level authorities for telework programs.

b. COMNAVRESFOR Director, Civilian Human Resources (N00CP) will:

(1) Provide Echelon II level program policy interpretation, advice, guidance and oversight.

(2) Oversee and coordinate COMNAVRESFOR implementation and administration of the civilian telework program.

(3) Prepare consolidated reports to DON and DoD on participation rates in the COMNAVRESFOR civilian telework program and other data, annually and as required.

(4) Designate a COMNAVRESFOR Civilian Telework Program Coordinator.

c. COMNAVRESFOR Deputy Chief of Staff for IT (N6) will:

(1) Provide Echelon II level IT policy, advice, guidance and oversight, as it pertains to the Civilian Telework Program.

(2) Renew and update the COMNAVRESFOR Information Technology Strategy, enclosure (1), as required.

d. Activity Heads/Commanders, or their Designees will:
(1) Determine if telework program is appropriate for their command.

(2) If determined appropriate, develop/implement telework procedures and policies consistent with this instruction and references (a) and (b).

(a) Review, approve or disapprove recommendations for denial of telework requests or cancellation of existing telework agreements. This authority may be further delegated.

(b) Make a final decision on telework requests within ten business days of receipt.

(c) Ensure justification for recommended denials or cancellations are based on sound business or mission related reasons.

(d) Report positions eligible to participate in the Civilian Telework Program to COMNAVRESFOR Director, Civilian Human Resources (N00CP), upon request.

(e) Designate a Command/Activity Telework Program Coordinator, if required.

e. Command/Activity Civilian Telework Program Coordinators will:

(1) Maintain copies of all approved, disapproved and cancelled Telework Agreements for one year.

(2) Gather information and respond to data calls on an annual or as-needed basis.

f. Supervisors will:

(1) Make position and employee eligibility determinations and report such determinations to the Command/Activity Civilian Telework Program Coordinator.

(2) Recertify position telework eligibility or ineligibility as part of the DON recruitment process.
(3) Notify employees of their eligibility to telework. Notify new hires of their eligibility to telework within two weeks of the report date.

(4) Assess or reassess telework agreements on an annual basis, or as needed.

(5) Recommend approval or denial of an employee’s request to telework within 10 business days. Recommendations will be routed through the chain of command for concurrence or non-concurrence to the designated approving official.

(6) Evaluate employee productivity for the time spent in a telework status.

(7) In emergency situations, administratively excuse the designated employee from teleworking, for extenuating circumstances, on a case-by-case basis.

(8) Complete the required training “Telework Training for DON Supervisors.” Training shall be documented in the Total Workforce Management System (TWMS).

(9) Ensure civilian employees complete and document in TWMS the required training “Telework Training for DON Employees,” prior to teleworking.

(10) For employees approved to telework, document approval on DD Form 2946 prior to start of the employee’s telework.

(11) Terminate telework arrangements if an employee’s performance or conduct does not comply with the terms of the telework agreement, or if the teleworking arrangement fails to meet organizational needs.

g. Eligible employees will:

(1) Submit request to telework, using form NAVRES 1000/8 and obtain approval to telework.

(2) If approved to telework, complete DD Form 2946, DEC 2011 and required telework training “Telework for Training for DON Employees” in TMWS prior to teleworking.
(3) Obtain and maintain adequate computer equipment and internet connectivity necessary to perform work from home. If the employee is working from an alternate government office, internet connectivity will be provided.

(4) Adhere to established telework policy instructions and required procedures. This includes required training, adhering to office procedures and protocol regarding when employees telework, where they can be reached and ensuring telework does not negatively impact their co-workers, immediate supervisor and customers.

(5) Account for work employees accomplish on a telework day/period.

(6) Ensure telework days and hours are properly accounted for in electronic time and attendance systems.

(7) Apply or reapply for telework program participation and complete telework training, on an as needed basis.

(8) Maintain the safety of the employee’s respective alternative worksite and report any injuries while working at the alternative worksite as soon medically practicable.

7. Participation.

a. Participation may be limited because of the duties encompassed by the position, operational needs, information technology requirements, staff coverage, employee performance, conduct concerns or other aspects of the work environment specific to the job in question.

b. Telework is meant to increase flexibility and productivity by maximizing resources. It is not to be used solely for the convenience of the participant.

c. Employees may not telework as a substitute for dependent care, e.g., child care or elder care.

8. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed per the Secretary of the Navy Manual 5210.1 of November 2007.

9. Forms. The following forms are available for download from the Navy Reserve Headquarters and Naval Forms web sites:

b. Commander, Navy Reserve Force Telework Request Form, NAVRES 1000/8, 5/14.

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

R. R. BRAUN

Distribution:
Electronic copy via COMNAVRESFOR Website
http://navyreserve.navy.mil
COMNAVRESFOR Telework Information Technology 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 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 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 (COMNAVRESPORCOM) 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 (SAAR) on file. Additionally, all users shall complete and stay current with their annual required DoD Information

Enclosure (1)
Assurance 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 COMNAVRESFORCOM. 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.


a. COMNAVRESFOR 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.

Enclosure (1)
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 COMNAVRESFORCOM 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. COMNAVRESFORCOM 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 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.

Enclosure (1)
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 email via OWA.** This is one of the primary telework uses for web access, which provides a version of the desktop email, contacts and calendar application. While some functionality is lost with OWA, including no 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. **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 capability (WiFi) 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. **WiFi,** which may include portable devices such as laptops, smartphones and tablets, come with built in WiFi wireless capability, requires the issuance of an NMCI WiFi card and associated software. Due to concerns over potential security exposures, use of WiFi is strictly limited to:

   (1) When in a public hot spot WiFi 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 Approving Authority-approved WiFi solution, hardware and software.

   Enclosure (1)
The use of a device’s native WiFi capability is not authorized.

(2) With the exception of access to OWA as per the OWA User Responsibilities and Acknowledgement, residential home WiFi 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.