COMNAVRESFOR INSTRUCTION 12610.2B

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
     (c) SECNAVINST 12271.1
     (d) 5 C.F.R Part 630

Enc./ (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) through (c). This instruction is a complete revision and should be reviewed in its entirety.

2. **Cancellation.** COMNAVRESFORINST 12610.2A.

3. **Collective Bargaining Agreements.** Provisions of an existing Collective Bargaining Agreements (CBA), memorandum of understanding (MOU), and/or memorandum of agreement (MOA) applicable to bargaining unit employees supersede the policies and procedures outlined herein unless to do so would violate any applicable government-wide law, rule, or regulation.

4. **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 recruitment and retention 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 facility and transportation costs, including costs associated with payment of the transit subsidy.

5. **Applicability**

   a. This policy applies to all Federal civilian positions and 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.

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

   a. Except as stated in the subparagraph (6)(f), entering into a telework agreement is voluntary on the part of the employee.

   b. Prior to commencing telework, eligible employees, as stated in subparagraph 7(f)(1), shall complete the Department of Defense (DoD) Telework Agreement (DD Form 2946) (12-11), required telework training depicted within the COMNAVRESFOR Telework Eligibility Checklist (NAVRES 1000/7) (05-14), and COMNAVRESFOR Telework Request Form (NAVRES 1000/8) (05-14) via the Total Workforce Management Services (TWMS), and submit to their supervisors and N00CP. All employees approved for telework shall adhere to the information technology (IT) strategy in enclosure (1).

   c. Telework requests will electronically be placed in TWMS, under Tools/Actions tab labeled, “Telework Request.” A new window will appear, “Create New Request,” click on create. Then the employee will agree to the DoD Terms of Telework Agreement and will abide by the rules and guidelines set within. If the employee has not completed DON Telework Training for Employees, or the employee has not taken the training in the last 2 years, he/she will be prompted to complete the mandatory training prior to completing the Telework Request. Once the training is recorded, TWMS will allow the employee to proceed with the telework request. Once completed online, the telework request will be sent to the supervisor of record for approval/denial.

   d. Employees desiring to telework shall follow procedures established by reference (a), this instruction, and their respective commands.

   e. Performance of duties while teleworking will involve only unclassified issues and material.

   f. Employees will not use personal computers or devices to telework unless they are using a MobiKey device or R2S (Ready-to-Serve) capable device. Employees can use a cellphone or tablet with R2S capability for situational telework only. Navy and Marine Corps Intranet
(NMCI) laptops are the preferred method for teleworking. Employees with a MobiKey device may utilize it for telework only until such time as a NMCI laptop is obtained. Prior to approval, supervisors must ensure all employees under a telework agreement have the proper equipment to perform telework. Employees can register for R2S at the following URL: https://private.navyreserve.navy.mil/cnrfc/N-Codes/N6/r2s/Pages/default.aspx.

g. During either natural or man-made emergencies or when continuity of operations (COOP) plans have been invoked, civilian employees who perform mission-critical duties may be required to work from home, at an alternate workplace, or from their regularly designated workplace to ensure continuity of operations and, if possible under the circumstances, 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 when weather conditions make commuting hazardous or circumstances arise that compromise employee safety (e.g., snowstorm, hurricane, act of terrorism, etc.).

h. Supervisors must ensure that 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 not worked. As an alternative, employees on maxi-flex work schedule may, with supervisor approval, flex their time on that day in accordance with reference (a). Supervisors may also approve employees’ request for use of appropriate leave during a period of unscheduled telework.

i. Under regulations outlined in reference (d), the Agency may grant weather and safety leave when it is determined an employee cannot safely travel to, or perform work at their normal worksite, a telework site, or other approved location because of severe weather or another emergency situation.

(1) Weather and safety leave is a form of paid time off authorized under the Administrative Leave Act. It will generally be used in conjunction with an operating status announcement issued by the Office of Personnel Management (OPM), DoD, DON, or the command. Under the law, weather and safety leave may not be granted to an employee who is
in a telework agreement and is able to safely perform telework at the employee’s home. This provision will apply regardless of what is stated, or not stated in the employees telework agreement and in applicable policies and agreements.

(2) The regulations provide that weather and safety leave may not be granted if the adverse conditions could have been reasonably anticipated. The employee is responsible for taking reasonable steps within his or her control to prepare to perform telework at the approved telework site.

7. 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 (DCHR) (N00CP) will:

(1) Provide echelon 2 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 Information Technology (IT) (N6) will:

(1) Provide echelon 2 level IT policy, advice, guidance, and oversight as it pertains to the Civilian Telework Program.

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

d. Activity heads/commanders or their designees will:

(1) Provide civilian employees the option to telework, once a determination has been made regarding eligibility of the position and the employee.
(2) Develop/implement telework procedures and policies consistent with this instruction and references (a) through (d).

(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 10 business days of receipt.

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

(d) Report telework eligibility determinations of positions and employees to COMNAVRESFOR DCHR upon request.

e. Command/Activity Civilian Telework Program Coordinators will:

(1) Maintain copies of all approved, disapproved, and cancelled telework agreements for 1 year following expiration or cancelation of the agreement.

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

(3) Provide copies of approved telework agreements to COMNAVRESFOR DCHR upon request.

f. Supervisors will:

(1) Make position and employee eligibility determinations, and report such determinations to the Command/Activity Civilian Telework Program Coordinator. Employees in positions that require, on a daily basis, direct handling of classified materials, on-site activity, or direct face-to-face communication are generally not eligible for telework. However, such positions could be still be determined eligible for recurring or situational telework (i.e., 1 day per pay period) provided alternate duties can reasonably be assigned on the telework day. Employees under formal DoD, DON, command training or entry programs; new employees receiving on-the-job training and interns are not eligible for telework.

(2) Recertify position telework eligibility or ineligibility as part of the DON recruitment process.

(3) Notify employees of their eligibility to telework and notify new hires of their eligibility to telework within 2 weeks of the report date.

(4) Assess or reassess an employee’s eligibility for telework on an annual basis, and as needed.
(5) Approve or recommend denial of an employee’s request to telework within 10 business days.

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

(7) In emergency situations, administratively excuse the designated teleworker 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 TWMS.

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

(10) For employees approved to telework, document approval on DD Form 2946 (12-11) prior to start of the employees telework, electronically through TWMS.

(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 and mission requirements. In such cases, the employee will be provided with the signed telework cancellation notice found in DD Form 2946 (12-11).

(12) Assist employees in obtaining necessary equipment such as NMCI laptops to perform telework.

(13) Ensure time spent in a telework status is accounted for and reported in the same manner as if the employee reported to duty at the official worksite. The Type Hour Codes for telework identified in the standard labor data collection and distribution application (SLDCADA) for documenting telework are TW for regular and recurring, TS for situational/ad hoc, and TM for approved medical reasons due to reasonable accommodation or workers’ compensation.

(14) If an emergency dictates a command dismissal, supervisors are required to notify their telework employees. Telework eligible employees will be required to continue their regularly scheduled work from the telework location. Employees who do not wish to continue to work may request leave.

g. Eligible employees will:

(1) Submit request to telework, using form NAVRES 1000/8 (05-14) and obtain approval to telework.
(2) If approved to telework, electronically complete DD Form 2946 (12-11) and required telework training “Telework for Training for DON Employees” in TMWS prior to teleworking. Employees will not be allowed to proceed with the telework agreement until the training is completed.

(3) Meet with their supervisor to review policy and to discuss and agree upon their individual telework requirements and assignments.

(4) Obtain and maintain adequate computer equipment and internet connectivity necessary to perform work from home. This includes having equipment necessary to telework when emergency conditions are expected. If the employee is working from an alternate government office, internet connectivity will be provided.

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

(6) Account for work they accomplish on a telework day/period.

(7) Ensure telework days and hours are properly accounted for $LDCADA. The Type Hour Codes are TW for regular and recurring, TS for situational/ad hoc, and TM for approved medical reasons due to reasonable accommodation or workers’ compensation.

(8) Apply or re-apply for telework program participation every 2 years and complete telework training on an as needed basis.

(9) Maintain the safety of their respective alternative worksite and report any injuries while working at the alternative worksite as soon medically practicable.

(10) Perform telework in an emergency situation as required by approved telework agreement or request leave as appropriate.

(11) Safeguard all DoD information, sensitive unclassified data, including Privacy Act or for Official Use Only data, and protect government furnished equipment (GFE).

(12) Immediately notify their supervisors if problems or issues are adversely affecting their ability to telework, such as equipment failure, power outage, phone/cable difficulties, etc. The supervisor has the right to request an employee to return to the office to complete work or the employee can request leave.

(13) During late openings/early dismissals, telework employees are expected to work their scheduled hours or request leave.
(14) During closures all telework eligible employees (regular/recurring and situational) are required to telework as a normal duty day at their telework location. Employees who do not wish to work may request annual leave.

8. Participation

a. Telework can only be initiated after all requirements stipulated in the preceding paragraphs are met, key points include:

(1) There are three types of telework:

(a) Regular/Recurring – Regularly scheduled each week or pay period, on the same scheduled days; normally not exceeding once per week or pay period.

(b) Situational – Approved on a case-by-case basis, can occur at any time, any day (health, weather, reasonable accommodation, and special projects). This also occurs when government offices are closed due to emergency event or when severe weather conditions or other circumstances disrupt commuting and compromise employee safety. Situational telework may be authorized for medical reasons (reasonable accommodation, worker's compensation, recovery from surgery/procedures). Medical documentation may be required to support a situational telework request.

(c) Emergency/COOP – Performed in an employee’s home or alternative worksite during a crisis situation or emergency event.

(2) Employees must be telework-ready, with approved IT and telephone equipment for telework. See subparagraph 6(f) for authorized IT equipment.

(3) The employee has completed the required training and telework agreement.

(4) The employee and supervisor have discussed and agreed to all rules regarding work to be accomplished.

(5) The supervisor will document approval or denial of the request within 10 business days. If the telework agreement is denied, the employee may escalate to the next level in their chain of command for final review and decision.

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

(7) Supervisors have the authority to recall an employee from a telework location at any time.
(8) Supervisors have the authority to cancel the employees telework day in advance and require the employee to report to the office.

(9) Employees teleworking must be available by phone or e-mail during the core hours of 0900-1430.

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

(11) Employees may not telework as a substitute for dependent care (e.g. child care or elder care).

9. **Termination of Telework Agreement.** The supervisor may terminate an employee telework agreement based on the law, mission requirements, office coverage, documented employee issues such as misconduct or unsatisfactory performance, disciplinary action within the past 12 months, unresolved security issues, official disciplinary action for being absent without permission for more than 5 days in any calendar year, and disciplined for viewing, downloading or exchanging pornography, include child pornography, on GFE, or while performing Federal Government duties.

10. **Telework as an Accommodation.** Requests to telework as reasonable accommodation are analyzed and evaluated under a different statutory authority than the Agency Telework Policy, Rehabilitation Act of 1973. For reasonable accommodations, please contact the Command Deputy Equal Employment Opportunity Officer.

11. **Testing Designated Positions.** Employees who are randomly selected while in an off-site telework duty status may be required to return to the official duty location, or may be granted a deferral for 60 days.

12. **Telework Day that Falls on a Holiday/Training or while in a Travel Status.** An employee is not entitled to a make-up day if his or her telework day falls during official training, holiday, or while in a travel status. A supervisor and employee, together, can agree to an alternate telework day if the mission of the command permits.

13. **Performance Standards.** Performance standards for telework ready employees must be the same as performance standards for non-telework employees. Expectations for performance should be clearly addressed in each employee’s performance plan, and the performance plan should be reviewed to ensure the standards do not create inequities or inconsistencies between telework and non-telework employees.

14. **Records Management.** Records created as a result of this instruction, regardless of media and format, must be managed per Secretary of the Navy Manual 5210.1 of January 2012.
15. Review and Effective Date. Per OPNAVINST 5215.17A, COMNAVRESFOR will review this instruction annually around the anniversary of its issuance date to ensure applicability, currency, and consistency with Federal, Department of Defense, Secretary of the Navy, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will be in effect for 10 years, unless revised or cancelled in the interim, and will be reissued by the 10-year anniversary date if it is still required, unless it meets one of the exceptions in OPNAVINST 5215.17A, paragraph 9. Otherwise, if the instruction is no longer required, it will be processed for cancellation as soon as the need for cancellation is known following the guidance in OPNAV Manual 5215.1 of May 2016.

16. Forms. The following forms are available for download on Navy Reserve Homeport and Naval Forms websites:

   a. Commander, Navy Reserve Force Telework Eligibility Checklist, NAVRES 1000/7 (05-14).
      https://private.navyreserve.navy.mil/cnrfc/Special_Assistants/N01A/Forms/Forms/AllItems.aspx

   b. Commander, Navy Reserve Force Telework Request Form, NAVRES 1000/8 (05-14).
      https://private.navyreserve.navy.mil/cnrfc/Special_Assistants/N01A/Forms/Forms/AllItems.aspx

   c. Department of Defense Telework Agreement, DD Form 2946 (12-11).

T. W. Lusher
Deputy

Releasability and distribution:
This instruction is cleared for public release and is available electronically only via COMNAVRESFOR Web site, https://www.mynrh.navy.mil/
This enclosure provides additional information on the info 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 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 e-mail accounts for FOUO, CUI, or PII transmission is strictly prohibited. E-mail sent containing FOUO, CUI, or PII data may only be e-mailed between Government e-mail 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 (COMNAVRESFORCOM) 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 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.

6. Government Furnished Equipment

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. 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. 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.

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, contacts, and calendar applications. 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. 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 networks 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.