DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

SECNAVINST 12271.1
ASN (M&RA)/OCHR
12 MAY 15

SECNAV INSTRUCTION 12271.1

From: Secretary of the Navy

Subj: DEPARTMENT OF THE NAVY TELEWORK POLICY

Ref: See enclosure (1).

Encl: (1) References
(2) Definitions
(3) Responsibilities
(4) Department of the Navy Information Technology Remote Access Capabilities and Limitations
(5) DON TELEWORK Information Technology Strategy Checklist
(6) Action

1. Purpose. To establish policy, assign responsibilities, and identify requirements for the Department of the Navy (DON) telework program. Guidance in this policy is in alignment and is consistent with the provisions of enclosure (1), references (a) through (r).

2. Cancellation. DON Civilian Human Resource Manual Subchapter 792.4, Appendix A, Work/Life, paragraph 4, Telework.

3. Definitions. See enclosure (2).

4. Applicability and Scope. This instruction covers Federal civilian employees and military service members. Service member applicability is determined at the discretion of the Chief of Naval Operations (CNO) and the Commandant of the Marine Corps (CMC). This policy does not apply to Federal contractors. Activities with local telework policies will review those policies and adjust as appropriate where there may be conflicts with this instruction. Bargaining unit employees will follow the terms and conditions of locally negotiated telework policies until such time as they may be modified through local negotiations.

5. Policy. The DON is committed to promoting and implementing telework to the greatest extent possible consistent with mission

capability and readiness. The DON telework program supports workforce efficiency, emergency preparedness, and quality of life. Telework is not an entitlement, but its use can serve as an effective recruitment and retention strategy, enhance DON efforts to employ and accommodate persons with disabilities, create cost savings by decreasing the need for extensive office space and parking facilities, and reduce traffic congestion, transportation costs, energy consumption, and pollution. It is DON policy to:

a. Execute responsibilities per enclosure (3).

b. Comply with the public law in reference (a) and the Department of Defense (DoD) policy in reference (b), including all DoD telework definitions and the exclusive use of the DD Form 2946, Department of Defense Telework Agreement, for all types of telework.

c. Determine telework eligibility status of all employees and determine position eligibility for telework using references (a) through (h) and notify employees accordingly.

d. Determine feasibility for each employee and position for regular and recurring telework (defined as a schedule of at least 1 day in a bi-weekly pay period) or situational/ad hoc basis for special assignments, inclement weather, or emergency telework situations and notify employees accordingly.

e. Authorize regular telework for eligible employees to the maximum extent possible that does not compromise the mission requirements. Mission requirements shall include consideration of the impact of telework on the DON remote access information technology (IT) network capacity and appropriate information security as outlined in references (f), (g), (i), (l), and enclosures (4) and (5).

f. Not allow telework for the following employees or positions:

(1) Employees in positions that require, on a daily basis, direct handling of classified materials.

(2) Employees in positions that require, on a daily basis, an on-site activity or face-to-face personal contact that

cannot be handled remotely or at an alternate workplace, e.g., hands-on contact with machinery or equipment, interns, new employees receiving on the job training, or direct face-to-face contact.

(3) Employees whose performance or conduct warrants more close supervisory direction as documented by the supervisor, whose rating of record is below fully successful, whose conduct has resulted in disciplinary action within the past 12 months, or who have unresolved security issues.

g. Allow the command's discretion on the length of time for which the employee is deemed ineligible for telework based upon criteria identified in paragraph 5f(1) through 5f(3) above.

h. Prohibit telework consistent with the eligibility guidelines set forth in references (a) and (b) if:

(1) The employee has been officially disciplined for being absent without permission for more than 5 days in any calendar year.

(2) Under reference (c), the employee has been officially disciplined for violations of subpart G of the Standards of Ethical Conduct of the Executive Branch for viewing, downloading, or exchanging pornography, including child pornography, on a Federal Government computer or while performing Federal Government duties.

i. Ensure Continuity of Operations (COOP) in remote work capability by practicing telework on a regular basis and maximizing the use of unscheduled telework for purposes of inclement weather per reference (j).

j. Provide the necessary equipment and office supplies for the use of government furnished equipment (GFE) for employees and service members who telework, within budgetary constraints, ensure fiscal responsibility by practicing cost effective options for remote access, and require supervisory pre-authorization for all telework related expenses.

k. Adhere to enclosure (4) and references (f) and (g).

l. Provide available assistive technology and services for telework usage free of charge to DON employees with hearing, visual, dexterity, cognitive, and communication impairments through the DoD Computer/Electronic Accommodations Program and provide procedural assistance with requests for reasonable accommodations for qualified person(s) with a disability as outlined in reference (r).

m. Require DON telework training for all teleworkers and supervisors of teleworkers prior to entering into a telework agreement. Document training completion in the position of record in the Total Workforce Management System (TWMS) or an equivalent system, but only if TWMS is not in use at that activity. Employees who are under an approved telework agreement on the date this instruction is signed do not need telework training consistent with the guidance set forth in reference (b).

n. Cover employees for work related injuries or illnesses while on official government business at the official worksite or at a telework site as required by references (d) and (e).

6. Responsibilities. See enclosure (3).

7. Action. See enclosure (6).

8. Records Management. Records created as a result of this instruction regardless of media or format shall be managed per SECNAV M-5210.1 of January 2012.

9. Reports and Forms

a. The DoD Annual Telework Report is assigned Report Control Symbol (RCS) DD-P&R(A) 243.

b. The SECNAV Telework Data Call is assigned SECNAV RCS 12271-1.

c. DD Form 2946, DoD Telework Agreement (DEC 2011) is available via the 'Forms' tab on the DoD Forms Management Web Site: http://www.dtic.mil/whs/directives/forms/index.htm.

d. SECNAV 12271/1, DON Telework Information Technology (IT) Strategy Checklist (FEB 2015) is available via the Naval Forms Online website at: https://navalforms.documentservices.dla.mil/web/public/home

RAY MABUS

Distribution: Electronic only, DON Issuances Web Site: http://doni.documentservices.dla.mil/

REFERENCES

(a) Public Law 111-292, Telework Enhancement Act of 2010
(b) DoD Instruction 1035.01 of 4 April 2012
(c) 5 CFR 2635.704
(d) 5 U.S.C. Chapter 81
(e) 33 U.S.C Chapter 18
(f) OMB Memo M-11-20, Implementing Telework Enhancement Act of 2010 IT Purchasing Requirements, of 28 April 2011 (NOTAL)
(g) OMB Memo M-11-27, Implementing the Telework Enhancement Act of 2010: Security Guidelines of 15 July 2011
(h) DoD Instruction 5200.01 of 9 October 2008
(i) DoD Instruction 8582.01 of 6 June 2012
(j) OPM Guidance, Washington, DC, Area Dismissal and Closure Procedures of December 2013
(k) SECNAVINST 12250.6A
(l) SECNAVINST 5211.5E
(m) SECNAVINST 12771.2
(n) SECNAVINST 5239.3B
(o) SECNAV M-5510.36
(p) DON CIO Memo, Policy for Issuance, Use, and Management of Government Provided Mobile (Cellular) Phone, Data Equipment and Services, and Calling Cards of 2 September 2005 (NOTAL)
(q) OCHR CHRM 1601, Equal Employment Opportunity of Jul 2005
(r) OCHR CHRM 1606, Procedures for Processing Requests for Reasonable Accommodations of Sep 2007

DEFINITIONS

These terms and their definitions are for the purpose of this Instruction.

1. Alternative worksite. A place away from the regular worksite that has been approved for the performance of assigned official duties. It may be an employee's or service member's home, a telework center, or other approved worksite.

2. Continuity of Operations (COOP) Planning. An effort to ensure that the capability exists to continue agency essential functions across a wide range of natural disasters or local or national declared emergencies.

3. Controlled Unclassified Information (CUI). Unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies.

4. Desk sharing. An arrangement in which two employees share the use of a single workspace where each employee has a designated date or time for use of this space.

5. Disciplinary action. Action taken to correct an employee's performance or conduct. These actions can range from written letters of reprimand to suspension, termination, or removal.

6. Eligibility. Characteristics of the job position and separately the employee, that identify suitability for teleworking as determined by the supervisor or other appropriate management officials in the employee's chain of command.

7. Emergency situation telework. Telework performed in an employee's or service member's home or alternative worksite during a crisis situation or emergency event by those employees or service members who perform duties in support of mission requirements during crisis situations or contingencies.

8. Employee. A DoD civilian employee, paid from appropriated or non-appropriated funds to include working capital funds and foreign national employees.

9. Federal Executive Board. A group composed of the heads of all Federal departmental and agency field offices, civilian and military, that is the primary means for distributing information, interagency training, and promoting discussion of Federal policies, activities, and management issues for Federal Executives in the field, e.g., agencies located in major metropolitan areas in the United States.

10. Hot desking. An arrangement in which employees use non-dedicated, non-permanent workspaces assigned on an unreserved first come, first-served basis.

11. Hoteling. An arrangement where employees use non-dedicated, non-permanent workspaces, assigned for use by reservation on an as-needed basis.

12. Official worksite. Approved location where the employee regularly performs his or her duties and is identified on the employee's SF-50.

13. Regular worksite. Location where an employee would work absent an alternative worksite arrangement.

14. Safe Access File Exchange (SAFE). An application for securely exchanging files up to 2GB. SAFE was created as an alternative file sharing method to email and file transfer protocol in order to send large files securely.

15. Situational telework. Telework that is approved on a case-by-case basis, where the hours worked were not part of a previously approved, ongoing, and regular telework schedule, e.g., telework as a result of inclement weather, medical appointment, special work assignments, or to accommodate special circumstances. Telework is also considered situational even though it may occur continuously for a specific period and is also referred to as episodic, intermittent, unscheduled, or ad hoc telework.

16. Supervisor. Civilian management official, commander, or service member who has responsibility for directing and managing employee work and for approving and denying employee telework agreements.

17. Telework. A voluntary work arrangement where an employee or service member performs assigned official duties and other authorized activities during any part of regular, paid hours at an approved alternative worksite, e.g., home, telework center, on a regular and recurring or a situational basis. Telework includes remote work where an employee resides and works at a location beyond the local commuting area of the employing organization's worksite. Telework does not include any part of work done while on official travel or mobile work, that is, work characterized by routine and regular travel to customer or other worksites instead of a single agency worksite, e.g., site audits, inspections, investigations, and property management.

18. Telework agreement. A written agreement, completed and signed by an employee and the authorized management official(s) via the DD Form 2946, that outlines the terms and conditions of the telework arrangement.

19. Telework center. A facility that provides a geographically convenient office setting with workstations and other office facilities and services that are used by civilian employees from more than one organization.

20. Telework site. Alternative worksite location where an employee or service member performs assigned official duties.

21. Unscheduled telework. A specific form of situational telework where an employee on an approved telework agreement performs assigned official duties at home or another approved worksite when Government offices are closed due to an emergency event or open, but severe weather conditions or other circumstances disrupt commuting and compromise employee safety.

RESPONSIBILITIES

1. Assistant Secretary of the Navy (Manpower and Reserve Affairs). Responsible for the issuance of telework policy and for delegations of authority within the DON.

2. Deputy Assistant Secretary of the Navy (Civilian Human Resources) (DASN (CHR)). Responsible for management, oversight, and administration of the telework program in the DON; and for providing authoritative advice to the Secretary of the Navy, the CNO, the CMC, and the heads of major commands.

3. Chief Information Officer (DON CIO). Responsible for providing enterprise strategy, policy, and oversight to ensure DON IT enterprise remote capabilities are properly managed and used within the constraints of DON IT infrastructure. The DON CIO shall:

a. Provide enterprise guidance and information on IT capabilities available to support telework and considerations in their use.

b. Establish acceptable use of policy to prevent unauthorized use of DON IT resources and information systems.

c. Establish policy for the protection of Personally Identifiable Information (PII).

d. Work with industry and Research, Development, Test and Evaluation Systems Commands and other appropriate sources to expand type and method of remote capabilities used.

DEPARTMENT OF THE NAVY
INFORMATION TECHNOLOGY REMOTE ACCESS CAPABILITIES AND LIMITATIONS

1. Overview

a. This enclosure provides additional information on the IT capabilities available to support DON telework. Understanding the advantages and disadvantages of the various technology options available for remote access will allow commands to make better informed decisions as they plan and budget for an increasing number of teleworkers.

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

c. Other remote access capabilities, such as Outlook Web Access (OWA) with smartcard readers, smartphones, etc. are viable alternatives for providing sufficient connectivity to support telework requirements. Commands shall advise their users of VPN capacity limitations and direct OWA and other remote access capabilities.

d. The ability to conduct business in a remote environment is critical to executing the mission of the DON. To maximize and protect this capability, users are reminded of their responsibility to practice good IT stewardship through responsible and effective use of DON IT resources. Whether connected from the office, home, or an overseas hotel room, unsafe practices provide a primary vulnerability to the overall health of the network and DON information.

e. Commands shall consult with their Command Security Manager in developing their telework program. The Information Assurance Manager (IAM) is the best source for current guidance on protecting government information, including information

defined as For Official Use Only (FOUO) and CUI. This guidance will be updated based on regular reviews of network impact.

f. Prior to authorizing telework, commands shall ensure users have training, an approved System Authorization Access Request on file, and a signed telework agreement (DD Form 2946). Additionally, all users shall complete and stay current with their required DoD Information Awareness and PII training annually, as a condition of continued access to the network.

2. Command Telework IT Strategy. All DON commands shall develop an IT Strategy Plan for telework. When developing a command telework IT strategy, commands must consider all available IT options, IT requirements best suited for the work performed, COOP plans, concurrent remote access network usage, equipment refreshing options, and the associated costs for remote access. When devising or assessing their plans, commands will consult with their IAM and Command Information Officer (IO) for the most current information on available telework IT options. New IT devices and capabilities are constantly being released into the marketplace and tested for DON network compatibility.

a. Command IOs will ensure that all GFE devices are configured to support telework per applicable DON and DoD information technology policies.

b. Command IOs will provide training as required to teleworkers on the various connectivity options available to them, including selecting the optimal Network Operations Center when VPN access is utilized.

c. Command IOs will maintain a copy of the command IT Strategy Plan for 2 years and assess trends, challenges, equipment refresh opportunities, and best practices for future plan development and implementation.

3. Government Furnished Equipment(GFE)

a. Regardless of the remote capability used, commands shall make every effort to provide the employee with GFE. The use of GFE 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 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.

c. Email containing PII must be digitally signed and encrypted. As an alternative, use of SAFE is available and authorized for transmitting PII. Details regarding the use of SAFE can be found on the DON CIO Web Site.

4. Personally-owned Equipment

a. Use of personally-owned equipment, such as a personal computer (PC), for telework is authorized as a last resort only when GFE is not provided or available. Hardware interface solutions such as mobiKEY allow for wider use of personally owned equipment.

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. The government cannot ensure that the optimal anti-virus and other software tools are installed on personal devices.

c. Mixing government and personal data on one device is discouraged. Storing any form of CUI, including PII, is prohibited on personally owned computers, mobile computing devices, and removable storage media. Processing or storing classified information on personal IT equipment is strictly prohibited.

d. Email containing PII must be digitally signed and encrypted.

e. 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 per current guidance on handling an electronic spillage, including the physical destruction of the hard drive.

f. The use of fax machines to send PII by DON personnel is prohibited.

g. Alternatives to the use of email and fax machines include the United States Postal Service and scanning. Scanned documents shall be transmitted using a secure means such as encrypted emails or SAFE. The use of SAFE is available and authorized for transmitting PII. Details regarding the use of SAFE can be found on the DON CIO Web Site.

5. Remote Access Capability

a. Commands should check with their local Customer Technical Representative to see what options are currently available for remote access.

b. The following is a list of common capabilities:

(1) A laptop is a fully-functional portable computer.

(2) A smartphone is a multi-function portable device that integrates a cell phone, Web browser, Microsoft Outlook, and other desktop applications on a pocket-sized device.

(3) A tablet is a touch or stylus-based device that provides smart-phone capabilities, except voice, with the benefit of a larger screen.

(4) A virtual desktop is a plug-in device that provides the user with a virtual representation of their government desktop computer on a personally-owned PC.

(5) A smart card reader is an external Common Access Card (CAC) reader that connects to a personally-owned computer via a USB port in order to support CAC login and authentication required for OWA and many official DoD sites.

6. 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.

Users should be provided with a hierarchy of connection options so that if the preferred connectivity method is unavailable they could try to connect with the next alternative in line. When providing GFE for a user, commands should also consider the various ways of connecting to the network and ensure the device is provisioned accordingly.

a. Web access 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 with a ".mil" domain.

b. OWA 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. OWA 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.

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 typically 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. Both may be available on any given device.

d. The number of VPN ports on the DON network is physically limited. Teleworkers without a bona fide need for VPN functionality to meet their job requirements should utilize OWA.

e. Portable devices such as laptops, smartphones, and tablets that may come with built in WiFi wireless capability,

require the issuance of an NMCI WiFi card and associated software. Due to concerns over potential security exposures, the following restrictions apply to the use of WiFi:

(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) Residential home WiFi networks are allowed when the network is set up per the current guidance from the DON CIO and the National Security Agency.

f. Cellular and/or Mobile Networks, such as DON BlackBerry devices and other approved GFE smartphones and tablets, generally connect through a commercial cellular network as their primary link to the network. Some BlackBerry devices supporting tethering should be utilized when available due to the significantly reduced cost of connecting a laptop to the device for Internet access instead of using an air card.

(1) United States based cellular providers generally provide a secure encrypted connection that supports remote access.

(2) Some foreign cellular networks are considered to be unsecure. It is important to contact your local IAM or Security officer for up-to-date travel guidance when taking a cellular or any wireless device overseas. Refer to the document "DON Guidance for the Use of Electronic Devices During Travel," available on the DON CIO Web Site.

7. On-line Resources. The following Web Sites contain the most recent information on IT topics of interest for telework.

a. NMCI Remote Access Options: https://www.homeport.navy.mil/home/

b. DON CIO Site: http://www.doncio.navy.mil/Main.aspx

c. DON Policy Issuances: http://doni.documentservices.dla.mil/

d. Federal Government Telework: http://www.telework.gov

DON TELEWORK INFORMATION TECHNOLOGY STRATEGY CHECKLIST

SECNAVINST 12271.1
SECNAV RCS # 12271-1

DON TELEWORK INFORMATION TECHNOLOGY (IT) STRATEGY CHECKLIST

Command Considerations	Employee Considerations
1. What will the office use as the primary means of communication for teleworkers? ☐ Email: Outlook Web Access (OWA), Air Card? ☐ Instant Message: Jabber (TWMS)? ☐ Laptop: Needed for PII, FOUO, or sensitive unclassified, or personal computer? ☐ Telephone: GOV, private, long distance calls? ☐ Video Teleconferencing: Defense Connect Online (DCO)?	1. Do you have the IT equipment necessary for the telework, and/or can you organize your work for cost effective use of office equipment? such as: ☐ Computing Device (personal or GOV) ☐ Internet Connectivity ☐ Air Card, Wireless Card, Tethering ☐ Phone - Smart, Desk, Cell ☐ Mobile Talon Card, SME PED ☐ CAC Reader ☐ MobiKEY, NMCI on a Stick ☐ Scanner or Fax Machine ☐ Web Camera, Audio Headset/Microphone
2. How will the office conduct meetings? ☐ Conference Calls, DCO, VTC, Telephone Bridge, or Direct Dial ☐ Audio headsets/microphones, web cameras?	2. Do you have the most current phone numbers for: ☐ Office Personnel ☐ Emergency recall purposes ☐ Help Desk Personnel ☐ Other? 2a. If "Other" please explain:
3. Are conference rooms equipped with an audio/telephone system that can ensure successful reception and transmission of voice conversations?	3. Do you have telecommunications voice or data plan that will economically accommodate high-frequency use?
4. Does the employee require full network access for telework?	4. If your primary means of connecting to the network to perform work is not available, do you have a backup plan?
5. What will the employee use to obtain a network connection (e.g., a local Internet Service Provider (ISP); Air Card; Wireless Card; or by tethering with a smartphone (i.e., Blackberry))?	5. Do you know how to establish and connect to virtual meetings or chat sessions?
6. If full access is needed: Has the employee been given a means to connect (e.g., Virtual Private Network (VPN) connectivity; "MobiKEY;" or "NMCI on a Stick")?	6. Have you forwarded your phone and/or do you know how to receive work phone calls and voice mail messages remotely?
7. If full access is not needed (no PII, FOUO, or sensitive unclassified): Have all software tools been provided to perform the work remotely?	7. Where will your data be stored and backed up? (e.g., Local hard drive; External disk; in the "Cloud").
8. Can the employee organize the remote work to reduce costs (in office equip. used for work)?	8. Have you been trained on the use of Data at Rest (DAR) encryption software?
9. Has the employee been issued a Common Access Card (CAC) reader?	9. Do you have access to all of the software you need to perform your work? (e.g., VZ Access to connect via VPN)

SECNAVINST 12271.1
SECNAV RCS # 12271-1

DON TELEWORK INFORMATION TECHNOLOGY (IT) STRATEGY CHECKLIST

10. How will you share and manage calendars?	10. If you are not using Government Furnished Equipment (GFE): ☐ Do you have anitvirus software installed and up to date virus signatures? (GOV antivirus software and updated signatures: https://infosec.navy.mil) ☐ Is your internet access configured in accordance with DON CIO Information Assurance for wireless or wired connection?
11. How will you manage share files? (e.g., via a web portal such a Defense Knowledge Online (DKO), Intelink; Navy Enterprise Portal (NEP) Command Site; or via direct network access)	
12. Does the employee have access to a fax or scanner and software that can generate editable documents?	
13. Can the Employee forward their desk telephones to an alternate location or access work voice mail remotely?	
14. Can employees sign and/or encrypt emails while teleworking to ensure authenticity and avoid spoofing?	

ACTION

1. The Director of the Office of Civilian Human Resources shall:

a. Provide guidance and assistance to the Echelon 1 and 2 Commands on telework program administration, implementation, and assessment.

b. Monitor and periodically assess the DON telework program and identify and address barriers to telework for maximum program effectiveness.

c. Maintain telework program metrics for effective measurement, assessment, and compliance evaluation as required by Congress and Office of Personnel Management (OPM).

d. Designate a DON Telework Managing Officer to assist with program implementation, coordinate with the DoD Telework Managing Officer to assess telework participation goal achievement, and submit reports as required to the OPM for the annual Status of Telework in the Federal Government Report to Congress.

2. The Secretary of the Navy, the CNO and the CMC shall:

a. Ensure this policy is implemented within their respective organizations.

b. Maintain situational awareness of remote access saturation points and direct changes in remote access capabilities as appropriate. Report to DON CIO any significant network degradation and mitigation.

c. Implement telework policies and procedures for service member eligibility and responsibilities per reference (b).

d. Ensure compliance with safeguarding requirements for classified and controlled unclassified information per DoDM 5200.01.

3. Heads of Echelon 2 Commands employing civilians shall:

a. Ensure subordinate commands and activities comply with statutes, regulations, guidance, and directions from higher level authorities, e.g., DASN (CHR), DoD, and OPM.

b. Implement the delegated authority for telework policies and programs, and ensure telework options are identified in the COOP.

c. Issue guidance and procedures to their subordinate commands and activities for internal program management to ensure maximum flexibility in program structure and command organizational mission requirements. Programs may include desk sharing, hot desking, and/or hoteling options.

d. Ensure that subordinate commands and activities are provided sufficient information technology, training, and program management resources to implement effective telework programs.

e. Establish and maintain annual telework participation goals, monitor goal progress, and identify and address barriers to telework for maximum program effectiveness.

f. Designate a command telework coordinator as a point of contact to OCHR to maintain effective telework program metrics for effective measurement, assessment, and compliance evaluation as required by Congress and OPM.

g. Ensure random drug testing requirements are addressed for employees in Testing Designated Positions by identifying how random testing will be handled if teleworkers are selected for testing while off-site, the provisions of local collective bargaining agreements, and the granting of testing deferrals.

h. Ensure that telework eligibility and implementation is equitably applied for equal opportunity employment.

i. Develop and implement an IT telework strategy plan that includes, but is not limited to, evaluating all available IT options, assessing IT requirements best-suited for the work performed, incorporating telework IT options into the COOP plan, evaluating IT equipment refresh options to contain associated IT

remote access costs, and assessing compliance with the DoD and DON information security IT policy (enclosure (4)).

j. Direct teleworkers to utilize the remote network access method that will provide sufficient functionality to perform their job with the least demand on network resources (see enclosure (4)).

4. Activity Heads and Commanders shall:

a. Ensure implementation of the telework program is in compliance with merit principles, laws, regulations, guidance, and direction from higher level authorities.

b. Ensure coverage of employees under an implementing instruction consistent with this policy and applicable regulations and procedures while reflecting the appropriate application of telework for the mission and type of work being performed.

c. Communicate telework program requirements to the workforce and provide DON telework computer based or classroom training and guidance to supervisors and employees. The DON telework on-line training courses will be used for employees and supervisors, at no cost to the organization.

d. Where appropriate and supportable, create employment and return-to-work opportunities by establishing telework for veterans, wounded warriors, persons with disabilities, military spouses, and injured workers receiving worker's compensation benefits.

e. Encourage the use of a situational and/or adhoc telework trial period of 6 consecutive pay periods in length consisting of 1 or more days of telework, prior to approving telework on a regular and recurring basis.

f. Ensure unscheduled telework is used per reference (j). OPM has jurisdiction for dismissal and closure announcements only for Federal employees working inside the Washington Capital Beltway in Washington, DC. Commands located outside the Washington Capital Beltway in Washington, DC may also use unscheduled telework as part of their emergency dismissal

procedures as directed by the commanding officer of the affected jurisdiction and reference (b) and/or in consultation with any local Federal Executive Board.

g. Within budgetary constraints, issue calling cards, provide cell phones, or reimburse for long distance (domestic or international) telephone expenses incurred in the performance of Federal Government work.

h. Designate an activity telework coordinator to define telework implementation procedures, respond to technical assistance inquiries from supervisors and employees, and submit required reporting data in a timely manner.

i. Conduct annual assessments on the telework program to identify and address barriers to equity of telework eligibility and application of remote telework through effective program evaluation.

j. Examine the use of telework to reduce costs associated with traditional office space real estate usage, greenhouse gas emissions caused by employee commuting, and improved productivity by effective absentee management.

5. Human Resource Offices shall:

a. Advise supervisors and/or employees on the proper execution of their civilian telework policy, procedures, and responsibilities.

b. Assist the heads of commands and activities in conducting the required reporting and self-assessments for their civilian telework program.

6. Managers and Supervisors shall:

a. Determine telework feasibility for employees consistent with the criteria outlined in enclosure (5).

b. Determine and designate all positions for telework eligibility, and ensure that eligibility is documented in the Defense Civilian Personnel Data System via My Workplace tool.

c. Participate in DON telework training prior to determining eligibility and approving or denying employee telework requests consistent with reference (b).

d. Approve, deny, or terminate employee telework requests or participation based upon the law, mission requirements, office coverage, documented employee misconduct, or unsatisfactory performance, as opposed to a preference for face-to-face supervision. Base denial of telework requests or eligibility on business reasons for mission requirements, performance, or the needs of the workgroup and justify, in writing, the basis for the denial or termination of telework on page 4 of the appropriate DD Form 2946.

e. Make decisions on telework requests within 30 calendar days, retain documentation for denied telework eligibility and approved requests, and retain all telework documentation, agreements, and supporting information for a minimum period of 2 years from the date of denial or approval.

f. Apply the same performance management standards for both teleworkers and non-teleworkers and ensure an equitable work environment for performance reviews, pay decisions, and promotions for both teleworkers and non-teleworkers.

g. Assure all teleworking employees and mission essential staff have completed and signed a DoD Telework Agreement Form 2946.

h. Per the Joint Travel Regulation, compensate travel costs between the alternative worksite and the official work site as identified on the employee’s SF-50.

i. Ensure that telework is not used as an alternative for dependent care.

j. Terminate telework agreements if an employee’s performance does not comply with the terms of the telework agreement or if the teleworking arrangement fails to meet organizational needs.

k. Ensure that employee locality pay is set using the definition of official duty station. Employees who are not required to report to a traditional work site at least twice in

each bi-weekly pay period will have their official duty station listed as their alternative work location and locality pay set accordingly. All other employees will have an official duty station of the traditional work location and have locality pay set accordingly.

l. Ensure teleworkers are accountable for GFE.

7. Employees shall:

a. Participate in DON telework training prior to entering into a telework agreement consistent with reference (b). Telework training is not required for employees who were teleworking with a telework agreement in place on the date this policy is signed.

b. Complete a DD Form 2946, DoD Telework Agreement as referred to in enclosure (3) of reference (b) and provide all requested information on the form.

c. Safeguard and ensure appropriate use of DON IT resources by protecting CUI and sensitive information as outlined in references (f), (g), (h), (l), and (n).

d. Assume responsibility for the installation, repair, and maintenance of all personally owned equipment and other incidental costs associated with a private residential remote worksite and operating costs including home maintenance, insurance, and utilities including any necessary phone and/or internet service.

e. Work at the traditional worksite on scheduled telework days if requested for mission requirements.

f. Contact the supervisor to request unscheduled telework when employees are offered this option per reference (j).

g. Maintain required performance critical elements and standards at the fully successful level or higher (or the equivalent).

h. Report telework in the appropriate time management system.

i. Maintain a safe work environment and immediately notify the supervisor if injured while teleworking.

j. Ensure that telework is not used as an alternative for dependent care.

8. Rights. Employees may challenge denied telework eligibility and denied telework requests through the administrative or negotiated grievance process, as appropriate, equal employment opportunity complaint process, and may use alternative dispute resolution (ADR) to resolve telework disputes through the DON Workplace ADR Program in conjunction with the above complaint process, where applicable.