



DEPARTMENT OF THE NAVY
CHIEF OF NAVAL PERSONNEL
WASHINGTON, D.C. 20370-5000

IN REPLY REFER TO

Canc: Oct 09
CHNAVPERSNOTE 5330
23 OCT 08

CHNAVPERSNOTE 5330

Subj: MANPOWER, PERSONNEL, TRAINING AND EDUCATION TELECOMMUTING
(TELEWORK) PROGRAM

Ref: (a) P.L. 106-346, Section 359 of 23 Oct 00
(b) Under Secretary of Defense Memorandum of 22 Oct 01
(NOTAL)
(c) Deputy Assistant Secretary of the Navy (Civilian
Personnel/Equal Employment Opportunity) Memo of
18 Dec 01 (NOTAL)
(d) DoD Instruction 1035.01 of 3 Apr 07
(e) DON CIO 291652Z Feb 08, (Subject: Loss of Personally
Identifiable Information Reporting Process)
(f) SECNAVINST 5239.3A

Encl: (1) Telework Approval Process
(2) Approved GSA Telework Sites in Washington DC
Metropolitan Area
(3) Transitioning to a Telework Environment
(4) IT Collaborative Tools
(5) Telework Agreement
(6) OWA User Responsibilities
(7) Remote Access Request

1. Purpose. To implement the Total Force Telework Program within the N1 domain based on the guidelines provided in references (a) through (f). This policy establishes a Telework program where eligible employees may participate in teleworking to the maximum extent possible without diminished organization or employee performance.

2. Background. Telework (also known as flexiplace, telecommuting, work-at-home) has emerged over the last decade in Federal government employment. This policy is a way to leverage technology while improving workforce efficiency and promoting workforce quality of life.

3. Objective. This program is designed to actively promote telework as a legitimate method to meet mission requirements for both military and federal civilian employees within the N1 domain. Enclosures (1) through (7) provide the structure and

OCT 23 2008

process to be followed to establish a successful telework program. The objectives of this program are to promote Navy as an employer of choice and improve the retention and recruitment of high-quality personnel. It also enhances efforts to employ and accommodate people with disabilities, including employees who have temporary health problems.

4. Policy. Telework is defined as an arrangement where a military member or a civilian employee (referred to throughout this notice as "employee") performs officially assigned duties at an alternative worksite on a regular and recurring or on a situational basis, also known as "ad hoc" telework. It is the Total Force policy that the maximum number of positions/employees be identified as eligible for regular and recurring teleworking (at least one-day per pay period, and ideally at least one-day a week) based on the criteria shown in enclosure (1). There are GSA Telework Centers available in some geographic areas that can be used by the civilian workforce at no cost to the activity. Enclosure (2) shows those available for personnel in the Washington DC metropolitan area. Similar centers may be available in other geographic areas. The following applies:

a. Supervisors and employees/members must follow the Telework Approval Process shown in enclosure (1) to this instruction.

b. Managers and Supervisors reserve the right to require personnel to report to the traditional worksite on scheduled telework days, based on operational needs and requirements.

c. Managers and Supervisors will continually review Telework arrangements to ensure continued effectiveness of participation in the program. Should the review indicate changes in effectiveness or employee/member performance, management can terminate the agreement with the employee at any time.

d. If the employee determines that the telework agreement is no longer beneficial to their quality of life, the employee may terminate the telework agreement.

e. Employees who are approved for telework are required to satisfactorily complete all assigned work per standards and guidelines in the employee's performance plan. Time spent in a teleworking status must be accounted for and reported in the

OCT 23 2008

same manner as if the employee reported for duty at the traditional worksite.

f. Overtime provisions that apply to civilian employees working at traditional worksites apply to civilian employees who telework. Employees may work overtime only when ordered and approved in advance by the supervisor.

g. All employees under a telework agreement must adhere to the Navy Information Assurance Instruction cited in reference (f) and ensure that his/her equipment is functional. Members must obtain at his/her expense, reliable and optimum connectivity to all necessary technology (internet access, phone, voicemail, or answering machine). If the member experiences any technology problems, he/she will notify their supervisor immediately and contact the appropriate service provider.

h. Telework can provide some valuable assistance with dependent care by saving commuting time. However, employees approved for telework shall not be engaging in care-giving activities during their assigned work times.

i. The employee/member understands and agrees that Navy will not financially reimburse them for routine business expenses pursuant to the Telework Agreement. CAC readers and applicable software will be provided, as necessary. Enclosures (3) and (4) provide information on business process review and IT Collaborative tools that should be considered to ensure success of Telework arrangements.

j. Consistent with DoD security and information technology policies no classified documents (hard copy or electronic) may be taken by teleworkers to alternate worksites. All materials and property provided by Navy are for authorized business use only. Security and care of Navy-supplied property and information are solely the employee/member's responsibility. The workforce will follow all DON CIO, N1 and NAVNETWARCOM policy, procedures and directives to protect all information, with a specific emphasis on preventing the presence of Privacy Act (PA) and Personally Identifiable Information (PII) in the Telework environment. Should Navy equipment be lost, stolen, or damaged, whether accidental or not, the member must report the incident immediately to the appropriate security officers and Branch Head. Should PA or PII data be lost or compromised, the


member must report the incident immediately to his/her Information Assurance Manager and follow procedures per reference (e).

k. Upon termination of the Telework Agreement, the employee must return all Navy property to their supervisor.

5. Responsibilities

a. Director, Civilian Personnel Programs (DCPP), OPNAV (N1T2) will serve as the advisor for the Telework Program within the MPTE domain and will provide and interpret DON and DoD policies on telework, as needed. N1T2 will update and revise this policy based on further guidance/direction from DoD or DON. N1T2 also serves as the OPNAV Telework Coordinator.

b. Each command within the N1 domain will appoint a Telework Coordinator to oversee and support telecommuting within the organization. The Telework Coordinator will be responsible for guiding the organization through telework implementation and retain all Telework Agreements in order to report annually on telework activity within the organization.


M. E. FERGUSON III
Vice Admiral, U.S. Navy

Distribution:

NETC

NPC

CNRC

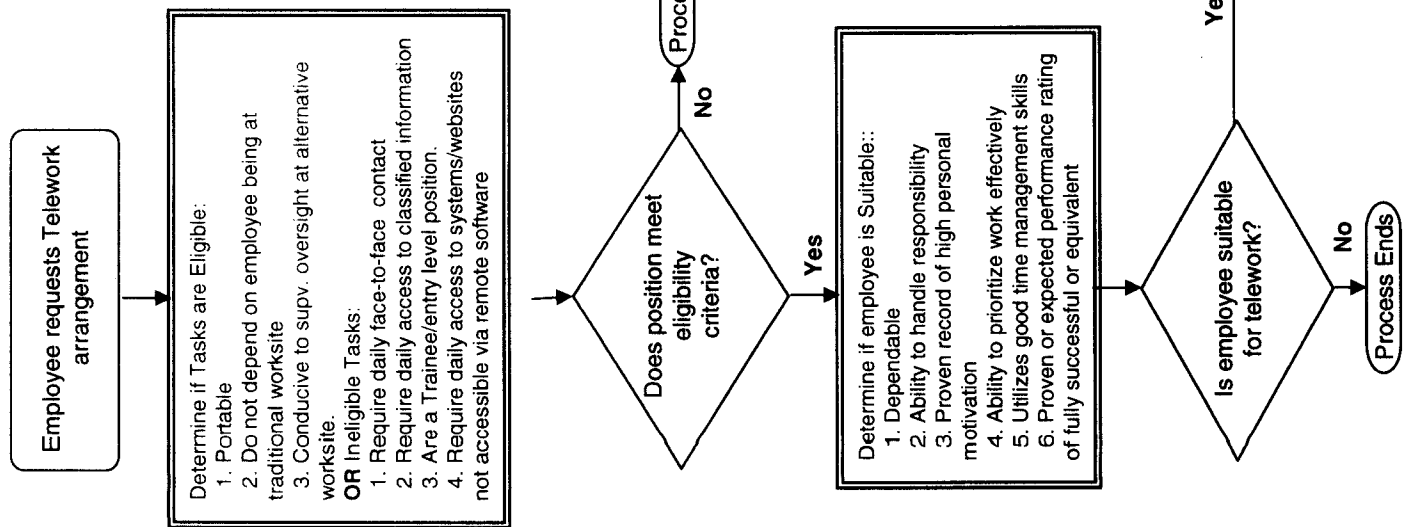
NSTC

All N1 Domain Commands

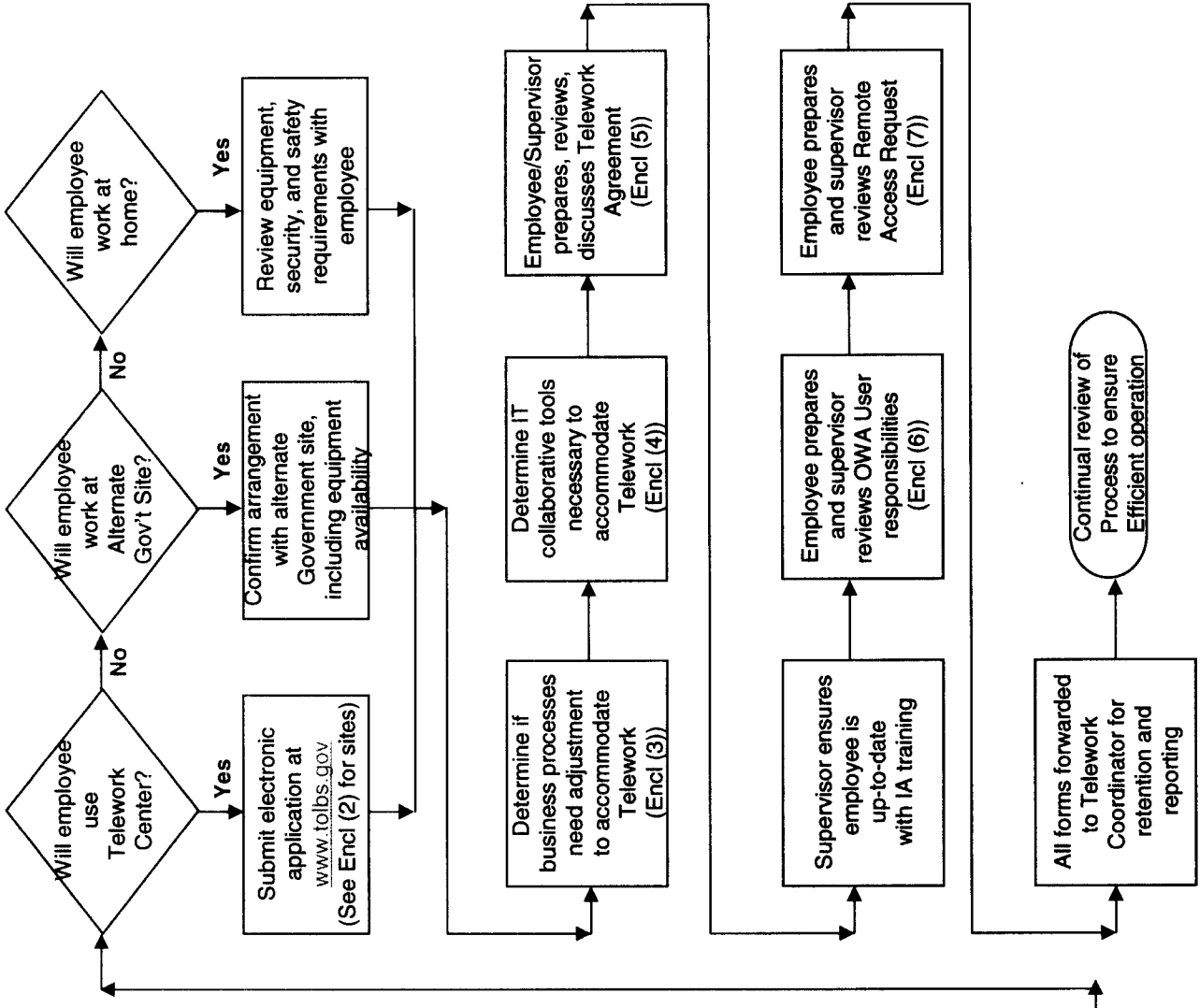
All N1 Division Directors

All N1 Special Assistants

Telework Approval Process



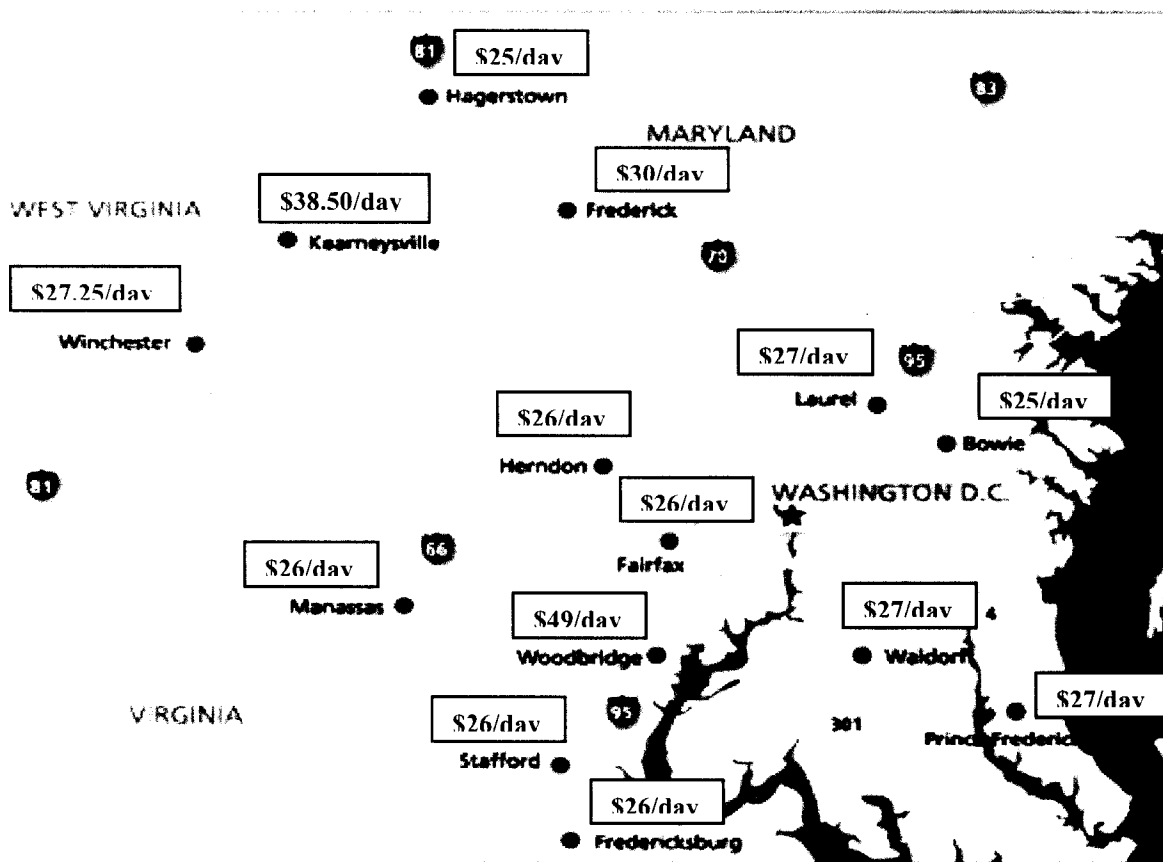
Enclosure (1)



TELEWORK CENTER LOCATIONS

As of May 6, 2008, the locations of the GSA Telework Centers in the Washington, DC commuting area are shown below. For those organizations outside of GSA, there is a daily rate charge which varies from location. The current rates are shown below. However, DoD assists with funding for civilians who use these centers.

Civilian employees interested in using a telework center as an alternate worksite should apply for use at: www.tolbs.gov. Follow the instructions provided to receive approval to use the facilities. All requests are on-line.



Transitioning to a Telework Environment

Telework can be advantageous to management and employees, if managed appropriately. It should be implemented strategically, taking into account the needs and work of the group, rather than granting or denying telework requests one by one. Employees should participate in the process and may be asked to help formulate possible solutions to issues that may arise.

Process Review

Managers should review their internal work processes to determine if processes need to be refined in order to facilitate telecommuting. For example, can files needed by all workers be secured in a file storage area that is accessible to the workforce whether they are in the office or at an alternate worksite?

Culture Change

Managers often ask, "How do I know what my employees are doing when I can't see them?" Performance standards for off-site employees are the same as performance standards for on-site employees. Management expectations of a teleworker's performance should be clearly addressed in the Telework Agreement. As with on-site employees, teleworkers must, and can, be held accountable for the results they produce. Good performance management techniques practiced by a manager will mean a smooth, easy transition to a telework environment.

Communicate Expectations

The Telework Agreement provided in enclosure (5) provides the framework for the discussion that needs to take place between the manager and the employee about expectations. For both routine and emergency telework, this discussion is important to ensure the manager and the employee understand each other's expectations around basic issues such as the following:

- How will the manager know the employee is present? (Signing in, signing off procedures may be needed.)
- How will the manager know the work is being accomplished?
- What technologies will be used to maintain contact?
- What equipment is the agency providing? What equipment is the teleworker providing?
- Who provides technical assistance in the event of equipment disruption?
- What will the weekly/monthly telework schedule be? How will the manager and co-workers be kept updated about the schedule? Do changes need to be pre-approved?

- What will the daily telework schedule be? Will the hours be the same as in the main office, or will they be different?
- What are the physical attributes of the telework office, and do they conform to basic safety standards? (Use a safety checklist.)
- What are the expectations for availability (phone, e-mail, etc.)?
- What is the expectation regarding the amount of notice (if any) given for reporting to the official worksite, and how will such notice be provided?
- How is a telework agreement terminated by management or an employee?

Facilitate Communication With All Members of the Workgroup

Teleworking and non-teleworking employees must understand expectations regarding telework arrangements, including coverage, communication, and responsibilities. Although individual teleworkers must take responsibility for their own availability and information sharing, managers should ensure methods are in place to maintain open communication across the members of a workgroup.

Remain Equitable in Assigning Work

Managers should avoid distributing work based on "availability" as measured by physical presence, and avoid the pitfall of assuming someone who is present and looks busy is actually accomplishing more work than someone who is not on-site. Good performance management practices are essential for telework to work effectively and equitably.

COLLABORATIVE IT TOOLS

There are various tools that allow for collaboration among workgroups and support a telework environment. The list below is not exhaustive, but provides some very useful tools to assist with a telecommuting workforce.

Remote Access Service (RAS): RAS allows employees to access their NMCI mail and files remotely using an NMCI provided laptop computer. Access requires the issuance of an NMCI compliant computer, associated Broad Band Remote Access Service (BURAS) training and approval for use. Information on RAS can be found at <https://www.homeport.navy.mil/support/topics/ras>.

Outlook Web Access (OWA): OWA allows employees to access their NMCI mail from anywhere. Access requires completion of training and approval of usage. Full information on OWA can be found at <https://www.homeport.navy.mil/search/?q=OWA>.

Navy Knowledge Online (NKO): NKO is an official Navy Website sponsored by the Naval Education and Training Command. It provides file storage that would allow your workforce to access files from remote locations. It also has instant messaging and "who's online" capabilities. Information on NKO can be found at <https://wwa.nko.navy.mil/portal/splash/index.jsp>.

Defense Knowledge Online (DKO): DKO is located on the Army Knowledge Online web site, but is available for all DoD services to use. It provides file storage that would allow your workforce to access files from remote locations. It also provides a quick access to Defense Collaboration Online (DCO) and has instant messaging and "who's online" capabilities. Information on DKO can be found at https://help.us.army.mil/cgi-bin/akohd.cfg/php/enduser/std_adp.php?p_faqid=119

Defense Connect Online (DCO): DCO is an IT tool that can be used to have a virtual meeting. It allows file sharing, online collaboration and changes to working documents, chat room during meetings, and voice communications through the computer (microphone required). There is no cost for DCO and it can be accessed at <https://www.dco.dod.mil/>.

OPNAV TELEWORK AGREEMENT

The following constitutes the terms and conditions of the telework agreement between:

Employee: _____

Last Name

First Name

Middle Initial

Title/Rank

Pay Plan

Series/ or Career Group
& Series for NSPS

Grade/or Pay Band for
NSPS

Activity/Org Code:
(e.g., 012 LR/ER)

Not all positions/individuals are eligible for telework. If the position/individual is not eligible for telework based on OPM's criteria (position requires access and/or handling of secure information, onsite staff, or the individual has a record of poor conduct and/or performance) the supervisor should deny the telework request by completing the block below. If the position/individual is eligible for telework, please proceed to the "Types of Telework" portion of this Agreement. Telework is NOT an entitlement.

INELIGIBLE POSITION- TELEWORK DENIED

The position/individual requesting telework is ineligible for telework because the position requires access and/or handling of secure information, onsite staff, or the individual has a record of poor conduct and/or performance, therefore the telework request is DENIED (state reason for denial).

Supervisory Signature

Denial

Date

TYPES OF TELEWORK

Regular and Recurring

yes no

Regular telework- an eligible employee works at least one day in a two week period with an approved work schedule and work location. If yes, please complete the work schedule below

Ad Hoc

yes no

Ad Hoc telework is when an eligible employee is approved to telework on an occasional, one-time, or regular basis. If yes, **DO NOT** complete the work schedule below, but maintain documentation of days and hours.

WORK SCHEDULES

The employee is approved to work at the alternative worksite below in accordance with the following schedule:

Please check the appropriate work schedule that the employee works (fixed or alternate).

For Civilians only:

Fixed

Alternate Work Schedule (AWS); if chosen, select from below types:

Compressed Work Schedule (CWS)

Flexible Work Schedule (FWS)

For ALL: Days in Biweekly Pay Period Employee is Authorized to Telework

Put a checkmark next to the day/days per week or day/days per every other week you will be teleworking.

DAY	PER WEEK	EVERY OTHER WEEK	DUTY HOURS <i>(specify hours of work that include lunch break, e.g., 0730-1700)</i>
MON	<input type="checkbox"/>	<input type="checkbox"/>	
TUES	<input type="checkbox"/>	<input type="checkbox"/>	
WED	<input type="checkbox"/>	<input type="checkbox"/>	
THURS	<input type="checkbox"/>	<input type="checkbox"/>	
FRI	<input type="checkbox"/>	<input type="checkbox"/>	
SAT			
SUN			

How many hours per pay period are you teleworking?

Alternative Worksite

The employee's alternative worksite is (please mark the appropriate checkbox and fill in the information):

Home office or work area

Address _____
Street City State Zip

Location of home office or work area (e.g., basement, upstairs room, etc.):
(update as necessary) _____

Phone Fax Official DOD Email

GSA Telecenter

Address _____
Street City State Zip

Phone Fax Email

Other approved alternative worksite:

Address _____
Street City State Zip

Phone Fax Email

Changes to Telework Arrangement

Employees who telework must be available to work at the traditional worksite on telework days on an occasional basis if necessitated by work requirements. Requests by the employee to change his or her scheduled telework day(s) in a particular week or biweekly pay period should be accommodated by the supervisor wherever practicable, consistent with mission requirements. A permanent change in the telework arrangement must be reflected in a new telework agreement.

Work-at-Home Telework

It is the responsibility of the employee to ensure that a proper work environment is maintained while teleworking.

Work-at-home teleworkers must complete and sign a safety and security checklist that proclaims the home safe for an official home worksite, to ensure that all the requirements to do official work are met in an environment that allows the tasks to be performed safely. The employee agrees to permit access to the home worksite by agency representatives as required, during normal working hours, to repair or maintain Government-furnished equipment, and to ensure compliance with the terms of this telework agreement.

For work at home arrangements, the employee is required to designate one area in the home as the official work or office area that is suitable for the performance of official Government business. The Government's potential exposure to liability is restricted to this official work or office area for the purposes of telework.

The employee acknowledges that telework is not a substitute for dependent care.

The Government is not responsible for any operating costs that are associated with the employee using his or her personal residence as an alternative worksite, including home maintenance, insurance, utilities, or internet/phone/long distance charges.

Official Duty Station

The official duty station for an employee covered by a telework agreement is the location of the regular worksite for the employee's position (i.e., the place where the employee would normally work absent a telework agreement), as long as the employee is scheduled to report physically at least once a week on a regular and recurring basis to that regular worksite.

The official duty station for an employee covered by a telework agreement who is not scheduled to report at least once a week on a regular and recurring basis to the regular worksite is the location of the telework site (i.e., home, telework center, or other alternative worksite), except in certain temporary situations. A change to the employee's official duty station may affect the employee's special salary rates and locality pay adjustments (market supplements). Review the following references prior to teleworking if a change of duty station relates to your telework situation:

OPM's Guide to Processing Personnel Actions - Chapter 23
Locality-based comparability payments - 5 CFR part 531, subpart F
Special rate schedules - 5 CFR part 530, subpart C
Cost-of-living allowances and post differentials, nonforeign areas - 5 CFR part 591, subpart B
Pay and Hours of Work OPM Fact Sheets

Note: If the employee's official duty station changes as a result of teleworking the employee and supervisor must sign the signature blocks on page 8 of the Agreement.

Time and Attendance, Work Performance and Overtime

Time spent in a teleworking status must be accounted for and reported in the same manner as if the employee reported for duty at the traditional worksite. There are no "carry over" of missed telework days. Annual and sick leave should be used for any personal needs. Telework is not to be used to conduct personal business.

The employee will share phone and email contact information with their office and be accessible during their scheduled work hours. The employee should check in at the beginning and end of the day and understand that they may be required to come to the office for face to face meetings during telework days.

The employee is required to satisfactorily complete all assigned work, consistent with the approach adopted for all other employees in the work group, and according to standards and guidelines in the employee's performance plan.

The employee agrees to work overtime only when ordered and approved by the supervisor in advance. Employees who work overtime without such prior approval may be subject to administrative or disciplinary action.

The employee agrees that he or she may be required to work at the alternative worksite on telework during emergency situations that may arise when the official duty station site is closed.

All employees that are identified as Continuity of Operations (COOP) essential onsite staff are required to have a telework contract.

Civilian employees will record their telework time in SLDCADA using the following codes:

Eh drop down field (environmental/hazard/other)

TW (telework regular)

TS (telework ad hoc/situational)

TM (telework medical)

Security and Equipment

No classified documents (hard copy or electronic) may be taken to an employee's alternative worksite. For regular and recurring telework, sensitive unclassified material, including Privacy Act and For Official Use Only data, may only be used by teleworkers provided with Government-furnished equipment. The employee is responsible for the security of all official data, protection of any Government-furnished equipment and property, and carrying out the mission of DOD at the alternative worksite. Government-furnished equipment must only be used for official duties and family members and friends of teleworkers are not authorized to use any Government furnished equipment.

Where the employee has been approved by the Component Designated Approving Authority (DAA) to use their personal computers and equipment for telework on non-sensitive unclassified data, the employee is responsible for the installation, repair and maintenance of all personal equipment. Employees must also obtain at their expense reliable and optimum connectivity to the internet, phone and either voicemail or an answering machine.

The employee agrees to adhere to NMCI Information Assurance policies and guidelines as well as all DON CIO and OPNAV policy, procedures and directives to protect all information with a specific emphasis on preventing the presence of privacy act (PA) and Personally Identifiable Information (PII) in the telework environment. Should PA or PII data be lost or compromised, the employee must report the incident immediately to their supervisor and to the Information Assurance Manager, following procedures in reference (e).

The Component is responsible for the maintenance of all Government-furnished equipment. The employee may be required to bring such equipment into the office for maintenance and should any of this equipment be lost, stolen or damaged, whether accidental or not, the employee must report the incident immediately to their supervisor and to the **appropriate security officers**. The NMCI Help Desk will provide support for hardware (CAC or laptop) and software (installation package). The employee must return all Government-furnished equipment and materials to the agency at the conclusion of teleworking arrangements or at the Component's request.

Liability and Injury Compensation

The Government is not liable for damages to the employee's personal or real property while the employee is working at the approved alternative worksite, except to the extent the Government is held liable by the Federal Tort Claims Act or the Military and Civilian Employees Claims Act.

The employee will not be financially reimbursed for routine business expenses pursuant to this Telework Agreement.

The employee is covered by the Federal Employees Compensation Act (FECA) when injured or suffering from work-related illnesses while conducting official Government business. The employee agrees to notify the supervisor immediately of any accident or injury that occurs at the alternative worksite while performing official duties and to complete any required forms.

Standards of Conduct

The employee acknowledges that he/she continues to be bound by the Department of Defense Joint Ethics Regulations, DOD 5500.7-R while working at the alternative worksite and using Government-furnished equipment.

Mileage Savings

The employee estimates that the telework arrangement will result in a reduction of approximately _____ miles traveled in commuting per week. (Do not complete this section if this Telework Agreement will result in a change to your official duty station.)

Termination of the Telework Agreement

Either the employee or the supervisor can terminate this Telework Agreement by giving advance written notice. Management shall terminate the Telework Agreement should the employee's performance not meet the prescribed standard, or the teleworking arrangement fails to meet organizational needs.

Telework Agreements must be reviewed and revised annually following the federal fiscal year October 1- September 30th.

Outside of the Continental United States

If teleworking outside of the continental United States, include cost estimates for overseas entitlements and the appropriate information security forms (i.e., signed User Awareness Agreement).

Pandemic Flu/Infrastructure Crisis

During a declared pandemic flu or infrastructure crisis, employees that are able to work may be directed to evacuate the work place and perform their work from an alternative work site or their homes (see 5 CFR 550.409).

Remote Access

Employees will fill out the attached Outlook Web Access (OWA) user agreement for remote access if using a home computer. Employees using government issued laptops, must obtain broad band remote access (BURAS) through their Activity Contract Technical Representative (ACTR).

Telework Training

Telework training is strongly recommended for both employees and supervisors. On-line training is available at www.telework.gov, and other telework information is available on the Work/Life pages at <https://www.Navyhr.navy.mil>

Other

Nothing in this agreement precludes the employee's management from taking any appropriate disciplinary or adverse action against an employee who fails to comply with the provisions of this Agreement.

Date of Commencement

The telework arrangement covered by this Agreement will commence on the following date:

(Telework shall not start until this Agreement is appropriately filled out, approved and signed by the requesting employee and supervisor, and submitted to the telework coordinator. Copies of the agreement should be kept by each.)

Employee Signature

By my signature, I certify that the information contained above is true and correct, and that I will abide by the terms and conditions of this Telework Agreement. Further, I certify that this Telework Agreement is in compliance with the most updated Telework Instruction, DoDINST1035.01(April 3, 2007), and understand that this agreement shall be reviewed and updated on a yearly basis beginning October 1st of each year. I understand that any modification to this information must be approved by my supervisor and submitted to the Telework Coordinator and/or Administrative Officer. I certify that classified documents will not be taken to my alternative work site. The supervisor will request an annual review and update in August or September with the employee and supervisor(s) to determine continuation of the agreement.

Employee Signature/Date

Supervisor Signature

I certify that the employee is eligible for telework according to the OPM criteria and will meet the requirements of his or her Position Description even though the employee will be working at an alternative worksite. Further, I certify that this Telework Agreement is in compliance with the most updated Telework Instruction, DoD INST 1035.01 (April 3, 2007), and understand that this Agreement shall be reviewed and updated on a yearly basis.

Supervisor Signature/Printed Name/Phone (Commercial/DSN)/Official e-mail address/Date)

NAVY Telework Coordinator approval is required before the Telework Agreement can be implemented for Washington DC telecenter usage. Electronic application for telecenters in the Washington DC metro area are located at www.tolbs.gov. Please contact your command telework coordinator for information and questions about telework.

THE FOLLOWING CERTIFICATION IS REQUIRED FOR TELEWORK IN WHICH THE EMPLOYEE'S OFFICIAL DUTY STATION WILL CHANGE:

I fully understand that any change to my Official Duty Station as a result of this Telework Agreement is for my sole convenience and benefit. Should my Official Duty Station change to an Alternative Worksite as a result of my request to Telework, I understand that I am not entitled to Permanent Change-of-Station (PCS) benefits or expenses under the DoD Joint Travel Regulations (JTR). I also understand change may affect my special salary rates and locality pay adjustments (market supplements). I further understand should this Telework Agreement be terminated by management or me, I am not entitled to PCS benefits or expenses under the JTR as a result of a change of the Official Duty Station back to my Traditional Worksite.

Employee Signature/Date

Supervisor Signature

I certify that the employee is eligible for telework according to the OPM criteria and will meet the requirements of his or her Position Description even though the employee will be working at an alternative worksite. I have explained to the employee that the change to the employee's duty station may affect the employee's special salary rates and locality pay adjustments (market supplements). Further, I certify that this telework agreement is in compliance with the most updated Telework Instruction, DoD INST 1035.01 (April 3, 2007), and understand that this Agreement shall be reviewed and updated on a yearly basis.

Supervisor Signature/Printed Name/Phone (Commercial/DSN)/Official e-mail address/Date)

PRIVACY ACT STATEMENT:

Authority: 5 U.S.C. § 301, Department Regulations; 10 U.S.C. § 5012, Secretary of the Navy, and P.L. 106-346 Section 359.

Purpose and Uses: To manage and administer the OPNAV Telework Program throughout the staff of the CNO/VCNO, DNS, N1, N2, N3/N5, N4, N6, N8 and N00 and to assist in the statistical reporting to the Department of Defense and Office of Personnel Management.

Effects of Nondisclosure: Personal information provided is given on a voluntary basis. Failure to provide the requested information may affect the processing of your request and may delay or prevent approval for teleworking under the DOD Telework Program.

SAFETY CHECKLIST (check appropriate answer)

1. Are temperatures, noise, ventilation, and lighting levels adequate for maintaining your normal level of job performance? YES NO
2. Is the electrical equipment free of recognized hazards that would cause physical harm (frayed wires, bare conductors, loose wires, or fixtures, exposed wiring on the ceiling or walls)? YES NO
3. Will the building's electrical system permit the grounding of electrical equipment (a three prong receptacle)? YES NO
4. Are aisles, doorways, and corners free of obstructions to permit visibility and movement?
YES NO
5. Are file cabinets and storage closets arranged so drawers and doors do not enter into walkways? YES NO
6. Are phone lines, electrical cords, and surge protectors secured under a desk or alongside a baseboard? YES NO
7. Is there a functioning smoke detector in the home? YES NO
8. Are you aware of the importance of working in an ergonomically correct manner – using a chair with back support; and having the computer monitor at eye level; keeping forearms close to parallel with the floor and your wrist fairly straight when typing?
YES NO

SECURITY CHECKLIST (check appropriate answer)

To assess the overall ability to protect Navy data and information processed, stored or transmitted or received at the home work site.

1. Do all doors and windows have adequate locking devices? YES NO
2. Is there a lockable file cabinet or container available to store documents? YES NO
3. Is the computer hardware positioned so unauthorized persons cannot see the screen?
YES NO
4. Does the computer have a keyboard or power supply locking device? YES NO
5. Are the computer and removable media adequately protected from unauthorized access? YES NO

6. When remotely accessing systems is your user password encrypted? YES NO
7. Have you received the annual Information Assurance training? YES NO
8. Do you possess an adequate working knowledge of how your computer transmits and receives data? YES NO
9. Do you possess an adequate working knowledge of what data needs to be protected when you transmit or receive data? YES NO
10. Are you familiar with computer virus detection and eradication procedures? YES NO

EMPLOYEE SIGNATURE

DATE

**OUTLOOK WEB ACCESS (OWA) USER RESPONSIBILITIES AND
ACKNOWLEDGEMENT
TO UNCLASSIFIED EMAIL**

Name (Last, First, M.I.)	Rank,	last 4	Dept/Div/Code
(Please print clearly)	Grade/Band	SSN*	

***PRIVACY ACT STATEMENT**

Account name

Phone

 Disclosure of this information is voluntary. However, nondisclosure shall result in denial of remote IT system access. Authority to request this information is contained in 5 U.S.C. § 301 for the purpose of requesting information to ensure that all military, civilian, and contractor personnel who have signed this security briefing/user Acknowledgement form are correctly identified. Also 10 U.S.C. Part II and 14 U.S.C. Chapter 11 provide authority for the Command Information Assurance Manager (IAM) to use the above data to ensure proper security indoctrination of all assigned personnel.

I understand or have completed, as applicable: (initial each)

___ I have completed OWA Web based training and have attached the training certificate. Training is available at: <https://www.homeport.navy.mil/training/owa/>. Select "NMCI Microsoft Outlook Web Access (OWA) Policy Training ver. 2.0" to complete the tutorial.

___ Using Outlook Web Access (OWA) poses risks to the network, some of which are described in the OWA Web-based training.

___ A demonstrated need, as certified by the Local IA (Command) Authority, is required for OWA use. Use of CAC-based PKI certificates is mandatory and must be installed on the non-DoD computer with high security enabled.

___ Use of personal firewall software, with port/protocol filtering features enabled, is required on the computer used to access OWA. Firewall settings are configured to "deny all" and allow by exceptions known applications. Government source software is available to support this requirement for all DoD employees and contractors as described at <https://infosec.navy.mil>.

___ Antivirus software and current virus signatures are installed and updated at least weekly on the computer used to access OWA. Managing the network health of the non-DoD computer is the responsibility of the user. Government source software and updated signatures are available to support this requirement

for all DoD employees and contractors as described at <https://infosec.navy.mil>.

___ Software patches for operating system and web browser are maintained current.

___ No peer-to-peer file sharing programs (e.g., Kazaa, Skype, Morpheus) shall be installed.

___ Password protection should be enabled on non-DoD computers to ensure family members or other unauthorized users do not inadvertently access OWA. Password-protected screen-lock will be set to activate within 15 minutes of inactivity.

___ Mail share programs are not allowed.

___ Ensure that no other wireless or LAN connection exists for the duration of the session. Any other existing connections must be disabled for the duration of the session. Except for the standard network interface device and directly connected printer, no peripherals should be connected while user is accessing OWA.

___ Users must delete all temporary internet files, close the browser and re-boot the non-DoD computer upon logging off OWA. Using Internet Explorer: Tools => "Internet Options" => General tab => "Delete files"

___ Use of OWA to access a NMCI account requires the user to adhere to all NMCI rules and procedures.

___ As a government OWA user I agree to unlimited government monitoring with no expectation of privacy from government authorities of my OWA designated account, whether at home, on travel, or my fixed government account.

___ Violations of this policy may result in loss of access privileges and/or disciplinary action. In addition, military, government, or contractor personnel may be subject to criminal penalties if they knowingly, willfully, or negligently violate this policy.

___ Sensitive Information and Personally Identifiable Information (PII) of others will not be stored or processed on non-DoD computers. In the event this occurs, the file

will be deleted before logging off and, where possible, overwritten (one overwrite is sufficient) using a utility available from DoD or major anti-virus vendors.

___ Prior to permanently leaving this command (e.g. transfer, retirement, separation, contract terminates), or if I no longer require OWA access, I agree to uninstall the middleware from my non-DoD computer and return the CAC reader to the appropriate person at my command.

___ OWA will not be accessed from public terminals such as libraries, colleges or airport/hotel business kiosks.

___ The following guidelines apply if classified information is found on the non-DoD computer (e.g. while using OWA):

- Disable and unplug all network connections.
- Do not transfer, copy, or forward any emails until the compromised classified information is fully sanitized or cleared as directed by member's command (IAM/Security Manager) or other appropriate authority.
- Do not attempt to delete or move to the trash bin any compromised classified information without explicit instructions or authorization from member's command IAM or other appropriate authority.
- Report the names of anyone else that may have also received or come in contact with the compromised information.
- Do not allow any family members or friends to come in contact or view the compromised information.
- If required, your local IAM or Security Manager may need to conduct a non-disclosure briefing.
- All E-mail messages created using OWA, sent or retrieved over OWA from a Non-DoD computer system are the property of the U.S. Government. The U.S. Government reserves the right to access the contents of any messages processed over its facilities if it believes such access is necessary for security, as evidence of violation of existing instructions or policy or to maintain good order and discipline. And if warranted, removal of the member's privately owned hard drive, floppy or storage device medias as necessary to safeguard and protect U.S. classified information.

By my signature below, I certify that I have read and understand this policy and agree to adhere to the direction contained herein. This form will be retained by the <COMMAND> IAM.

Signature: _____ Date: _____

System Serial Number(s) of Non-DoD computer(s):

Location: _____ Laptop: yes / no (circle)
(City/State)

5230
DD Mon YY

From: _____ (requestor)
To: Local IA Authority
Via: Branch head (NCODE): (Signed) _____

Subj: REQUEST FOR REMOTE ACCESS TO UNCLASSIFIED E-MAIL BY
A NON-DOD COMPUTER

Encl: (1) OWA User Responsibilities and Acknowledgement
(2) OWA Training Completion Certificate

1. I have read, understand and signed enclosure (1) and completed Outlook Web Access (OWA) training provided by Navy Marine Corps Intranet (NMCI) available at the NMCI Homeport <https://www.homeport.navy.mil/training/owa/>.

2. I have attached my certificate of completion as enclosure (2).

3. I am requesting remote access capability to unclassified e-mail account:
_____@navy.mil.

4. I require access for the following reason(s):

5. I have installed and maintain both the antivirus software and signatures current on the computer(s) I use to access OWA. I have installed and maintain a firewall on (or protecting) the computer(s) I use to access OWA.

Requestor signature

Enclosure (7)