VPN / Wi-Fi REMOTE ACCESS REQUEST

Authority: Executive Order 10450, 9397; Public Law 99-474; the Computer Fraud and Abuse Act; 5 U.S.C Statute 301; 10 U.S.C. Part II; 14 U.S.C. Chapter 11; UCMJ;
DOD 5500.7R, Joint Ethics Regulation; CJCSM 6510.05, SECNAVINST 5239.3A, DON Information Assurance (IA) policy, and E.O. 9397; NETWARCOM message
311452ZMAR2005 and DON CIO message 161957ZOCT02 Remote Access To Enterprise Email From non-DoD Computers.

Privacy Act of 1974 Statement: This Regulation is reissued under the authority of DoD Directive 5400.11, "DoD Privacy Program," May 8, 2007 (Reference (a)). It provides guidance on section 552a of title 5 United States Code (U.S.C.), the Privacy Act of 1974, as amended, (Reference (b)), and prescribes uniform procedures for implementation of the DoD Privacy Program.

ONE-Net UNCLASSIFED VPN Policies and Procedures:

Purpose:

To ensure that the undersigned requester fully understands the very intent of the policies and procedures of ONE-Net and with respect to CLASSIFED and UNCLASSIFED VPN solutions, either explicitly detailed or implicitly implied.

Responsibilities:

Undersigned requester, having already been authorized to access the ONE-Net enclave by approval of a SAAR-N form, agrees to, and understands the following fundamental, but not limited policies and procedures with respect to permitted access and usage of UNCLASSIFED VPN solutions:

Naval Information Forces ONE-Net user VPN Enablement Policies and Procedures:

1. As set forth in CTO 08-005 and NETWARCOM Naval Telecommunications Directive (NTD) 06-06, requester will remain in compliance with user agreement(s) and/or responsibilities stated in OPNAV 5239/14, System Authorization Access Request Navy (SAAR-N). This includes all terms and conditions stated in the SAAR-N when utilizing an authorized VPN/Wi-Fi solution.
2. The requester will, on an annual basis, show a need for continued use of VPN/Wi-Fi access per the DON CIO Acceptable Use of DON Information Technology, 12 February 2016.
3. Requester understands that ONE-Net will routinely intercept, record and/or monitor any or all communications for the purposes of, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations security which encompass the defense of aforementioned operations, personal misconduct, law enforcement investigations, and counterintelligence investigations. The information or data should therefore not be considered as private.
4. Requester will immediately report any security violations, unintentional CLASSIFED information spillage and/or suspicious Information System activity to their immediate supervisor, the local site's ONE-Net Information Systems Security Manager (ISSM) and/or Information Systems Security Officer (ISSO), Command Security Manager (CSM) and/or the Enterprise Service Desk (ESD).
5. Requester acknowledges, understands and consents that at any time, any authorized member of the US Navy Information Assurance organization, US Naval command authority officials, and/or law enforcement agencies may monitor, record, request to inspect and/or seize suspected personal computer(s), external hard drives, flash/thumb drives, and stored data on a DoD Information System(s) and/or its associated equipment that include, but are not limited to, personal property connected to and/or used in conjunction with access to a DoD Information System in the viewing and/or storage of aforementioned information.
6. Responsible for all actions taken under the level of access for which they have requested and been authorized.
7. Protection of all associated access passwords and PINs at the highest level of data they secure.
8. Properly protect and label all output to include printouts, CDs and DVDs and/or other various forms of media, Privacy Act data and other protected Personally Identifiable Information (PII) while it is processed and/or at rest.
9. Ensure the use of Logout function and closure of browser windows when terminating VPN connections.
10. Prohibited is the introduction of CLASSIFED information into an UN CLASSIFED environment or information system.
11. Prohibited is the access, storing, processing, displaying, distributing, transmitting, or viewing of any material(s) that may be deemed as: abusive, harassing, defamatory, vulgar, pornographic, racist, and/or promotes hate crime, or is otherwise subversive in nature.
12. Prohibited is the violation of any established security and/or protection policies which have been identified as: CLASSIFED, Proprietary information, Controlled UNCLASSIFED Information (CUI), For Official Use Only (FOUO), or related to PRIVACY ACT of 1974 statement information; while viewing handling, storage, processing, distributing and/or transmittal of aforementioned data.
13. Prohibited is the access of VPN using public or privately-owned computers.
14. Prohibited is the access of VPN solutions and simultaneous use of Wi-Fi enablement, Peer-to-Peer sharing of files, video games, on-line streaming video, installation, transfer, copying, pasting, or obtaining of any software or media in violation of a vendor(s) patents, copyright, trade secret(s), or licensing agreement(s).

Naval Information Forces ONE-Net User WI-FI Enablement Policies and Procedures:

1. I will protect controlled UNCLASSIFIED information to prevent unauthorized access, compromise, tampering, or exploitation.
2. I will immediately report all information security incidents (lost, theft, involuntary disclosure, etc.) in accordance with local procedures, CJCSM 6510.01 (series) and SECNAV M5510.36A to the Site/Regional Information Systems Security Manager and/or Security Manager.
3. I will inform the Information Systems Security division in the event that my desk location changes and/or the use of the hardware is required at a different location.
4. I am aware that USB Wi-Fi technology is provided to enable mobile networking, such as telework or travel, however it is neither designed, nor is it approved for use in Department of Navy (DON) spaces.
5. I am aware that funding of the USB wireless adapters will be the responsibility of the users Commands. All charges incurred due to the wireless networks will be the sole responsibility of the approved user of the PC and wireless adapter or the users Command depending on command policy.
6. I am aware that I must use approved USB Wi-Fi devices that are listed on the ONE-Net APL.
7. I am aware that users issued devices with USB wireless technology must be aware of and acknowledge the above requirements as an addendum to the System Authorization Access Request-Network (SAAR-N) form.
8. I am aware prior to entering any secure spaces users shall remove the USB wireless adapter from their PC.
9. Custody change from user to user without proper documentation is strictly prohibited. All custody changes must be authorized by the Command ISSM/ISSO.
10. Willful or negligent violation of this document are subject to disciplinary action under the Uniform Code of Military Justice or criminal penalties under applicable federal statute, as well as, administrative sanctions.

*** Form must be retained by the requesting unit/command IAW current SAAR-N OPNAV 5239/14 section E Disposition of Form. Form may be maintained by the Navy, requesting user's ISSM, and/or Security Manager. Completed forms contain Personal Identifiable Information (PII) and must be protected as such.**

☑	**I am requesting VPN authorization and access to the ONE-Net enclave. And I HAVE READ, ACKNOWLEDGE AND UNDERSTAND the VPN access Policies and Procedures in its entirety** **(VPN is only authorized for UNCLASSIFIED access)**
☑	**I am requesting Wi-Fi authorization and access to the ONE-Net enclave. And I HAVE READ, ACKNOWLEDGE AND UNDERSTAND the Wi-Fi access Policies and Procedures in its entirety.** **(Wi-Fi is only authorized for UNCLASSIFIED access)**

1.) TYPE OF REQUEST	2.) DESIGNATION OF REQUESTOR	3.) TYPE OF ACCESS	4.) COMMAND	5.) DEPARTMENT/DIVISION
INITIAL	MILITARY	UNCLASSIFIED	CNRJ	

6.) REQUESTOR'S NAME (Format – Last, First, Middle)	7.) REQUESTER OFFICIAL (.MIL) EMAIL

8.) JUSTIFICATION FOR ACCESS	9.) DSN PHONE (Area Code + 7 Digits)	10.) COMMERCIAL PHONE (Format – enter number after + (add dashes))
To perform official Government work duties.		

11.) VPN ONE-NET LAPTOP INFORMATION **Requester understands: Only Government-owned workstations are approved for VPN access and are subject to re-inspection every 30-days.**

11a.) MAKE	11b.) MODEL	11c.) SERIAL NUMBER	11d.) MAC ADDRESS
HP			

12.) ONE-NET WI-FI HARDWARE INFORMATION **Enter Wi-Fi hardware information.**

12a.) MAKE	12b.) MODEL	12c.) SERIAL NUMBER

13.) REQUESTOR (DIGITAL ONLY) SIGNATURE	14.) DATE (Format – dd-mmm-yyyy)

15.) REQUESTOR'S N6 (or equivalent) NAME (Format – Last, First, Middle)	16: DSN PHONE (Area Code + 7 Digits)	17.) DATE (Format – dd-mmm-yyyy)

18.) REQUESTOR'S N6 (or equivalent) (.MIL) EMAIL	19.) REQUESTOR'S N6 (or equivalent) (DIGITAL ONLY) SIGNATURE