ONE-NET ENTERPRISE OUTLOOK WEB ACCESS (OWA) USER ACKNOWLEDGEMENT FORM

PRIVACY ACT STATEMENT

AUTHORITY:	Executive Order 10450, 9397; Public Law 99-474; the Computer Fraud and Abuse Act.
DISCLOSURE:	The information below may be used to identify you and may be disclosed to law enforcement authorities for investigating or prosecuting a violation of the law. Disclosure of information is voluntary; however, failure to disclose information could result in denial of access to OCONUS Navy Enterprise Network (ONE-NET) Information Technology (IT) resources.
PRINCIPAL PURPOSE:	To record names, signatures and other Personally Identifiable Information for the purpose of validating the trustworthiness of individuals requesting access to ONE-NET OWA systems. NOTE: Records may be maintained in both electronic and/or paper form.

POLICY STATEMENT

AUTHORITY:	The use of this OWA User Acknowledgement Form including the terms and conditions stated is in accordance with 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.
PRINCIPAL PURPOSE:	To emphasize individual responsibilities pertaining to the operation, administration, management and control of all personal computers and government-owned computers while utilizing Outlook Web Access. Ensure the user is aware of their responsibilities to ensure the protection of any information accessed through OWA is based on the principles of individual responsibility, personal accountability and need-to-know.

1. TYPE OF REQUEST □ INITIAL □ MODIFICATION □ DEACTIVATE	2. ONE-NET USER LOGON NAME(S) < UNCLASS __________ CLASS __________

PART I - REQUESTOR INFORMATION

3. NAME (*Print Last, First, Middle Initial*)	4. SSN (*Last 4*) or ID #	5. PHONE (*DSN or Commercial*)
6. COMMAND UIC / PLA	7. OFFICE SYMBOL/DEPARTMENT	8. BUILDING NUMBER / ROOM NUMBER
9. OFFICIAL MAILING ADDRESS	10. JOB TITLE AND GRADE/RANK	
	11. CITIZENSHIP □ US □ FN *List country below* □ OTHER ________	12. DESIGNATION OF PERSON □ MILITARY □ CIVILIAN □ CONTRACTOR □ FNIH
13. PARENT ORGANIZATION / ORGANIZATION	14. PCS / DEPARTURE DATE (*YYYYMMDD*)	15. DATE (*YYYYMMDD*)

PART IIa - USER AGREEMENT (Acknowledgement and Understanding of Risks Associated with OWA Use)

16. OWA is provided for the conduct of official business while not directly connected to ONE-NET. The inherent risk of using this public source should be appreciated by all ONE-NET users. The requestor understands the risks and actions required to take as identified below.

1. After completing use of OWA, it is imperative that the requestor ensure that selection of Logout and the closure of all browser windows is taken. If these actions are not taken, it may allow an attacker to use the system to resume the requestor's OWA session.
2. It is possible that a classified data spillage may occur through the use of UNCLASSIFIED OWA. This may occur inadvertently by simply opening an email or downloading an attachment containing CLASSIFIED information. As a result, there are significant consequences as stated in Part IIc.
3. Storage of passwords used to access PKI certificates or provide user account authentication for OWA on the system being used to access OWA from may allow an attacker to utilize the requestor's credentials and access to OWA.
4. Protection of the ONE-NET user account is essential. The requestor will be held responsible for the use of the user account for any attempted or successful probes or break-ins to OWA, its related systems or other ONE-NET systems or accounts; internal protection circumvention, accounting or auditing defeating tactics; or the use of OWA related systems and assets for purposes other than which they were intended or accredited. Any of these activities will be reported as security violations and may result in disciplinary action in accordance with the UCMJ or civilian disciplinary rules, as appropriate.

Requestor Initials ________

PART IIb - USER AGREEMENT (Terms and Conditions for CLASSIFIED OWA Use)

17. The following rules outlines basic safeguards that must be closely followed when accessing the CLASSIFIED OWA application and its related systems. Refusal to agree to these terms and conditions will prohibit the requestors authorized access to CLASSIFIED OWA. The requestors initials at the bottom of this block signifies acknowledgement of the following:

1. Requestor will remain in compliance with NETWARCOM Naval Telecommunications Directive (NTD) 06-06 mandated use of the Navy version of DD FORM 2875, SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR). This includes all terms and conditions stated in the SAAR specifically Block 27 - additional information section - when accessing OWA. If the SAAR has not yet been signed according to NETWARCOM NTD 06-06, the requestor will follow all rules stated in the ONE-NET regional/site user agreement form signed in addition to those stated in the SAAR.
2. Requestor will maintain demonstrable need to access CLASSIFIED OWA
3. Requestor will immediately report any ONE-NET IT asset security violation, inappropriate or suspicious user/system activity to the site's ONE-NET Information Assurance Manager (IAM) and Regional Service Desk.
4. Access to CLASSIFIED OWA is only permitted from an accredited SIPRNET system.
5. Requestor will not store CLASSIFIED data on the machine used to access CLASSIFIED OWA from unless it can be ensured that users of that system have need-to-know.
6. Requestor will maintain a SECRET or above clearance and valid need-to-know. Requestor will report any changes to either condition immediately to the local site ONE-NET IAM.

Requestor Initials ________

NAME *(Last, First, Middle Initial)*	DATE *(YYYYMMDD)*	SSN or ID #

PART IIc - USER AGREEMENT (Terms and Conditions for UNCLASSIFIED OWA Use)

18. The following rules outlines basic safeguards that must be closely followed when accessing the UNCLASSIFIED OWA application and its related systems. Refusal to agree to these terms and conditions will prohibit the requestors authorized access to UNCLASSIFIED OWA. The requestors initials at the bottom of this block signifies acknowledgement of the following:

1. Requestor will remain in compliance with NETWARCOM Naval Telecommunications Directive (NTD) 06-06 mandated use of the Navy version of DD FORM 2875, SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR). This includes all terms and conditions stated in the SAAR specifically Block 27 - additional information section - when accessing OWA. If the SAAR has not yet been signed according to NETWARCOM NTD 06-06, the requestor will follow all rules stated in the ONE-NET regional/site user agreement form signed in addition to those stated in the SAAR.
2. Requestor will maintain demonstrable need to access UNCLASSIFIED OWA.
3. Requestor will immediately report any ONE-NET IT asset security violation, inappropriate or suspicious user/system activity to the local site's ONE-NET Information Assurance Manager (IAM) and Regional Service Desk.
4. Only a U.S. Government-owned asset, contractors' company provided computers, or a ONE-NET user's privately owned computer may be used to access OWA. Computers belonging to friends or relatives shall not be used.

When using a non-U.S. government computer the following conditions also apply:
1. OWA shall not be accessed from public terminals such as library, university, airport or hotel kiosks nor shall it be accessed from non-government owned handheld Personal Electronic Devices (PEDs).
2. If the requestor is not the sole user of the non-U.S. government computer, steps must be taken to prevent the other users of the privately-owned computer from purposely or inadvertently accessing data obtained through the use of OWA or accessing OWA itself. The operating system in use on the privately-owned computer must support multiple account access. This is limited to Windows NT, XP, 2000 and Windows Vista; Linux (includes Apple Mac with OS X or higher) and UNIX. Windows OSs shall use the NTFS file system and other OSs shall ensure ACLs limit access to the requestor's user account directories. The requestor shall ensure any files obtained through OWA are stored in folders that the other users cannot readily access. Also, the requestor shall be the only person with administrative privileges on the computer and ensure a strong password (DoD password complexity compliant) is used and is not known to anyone else. The administrative account shall be used only when absolutely necessary (e.g. to install software). Non-approved handheld devices are not permitted to access OWA.
3. Must use Personal/desktop Firewall software (e.g. Symantec Firewall, McAfee Desktop Firewall, Windows Firewall) when using any connection type (e.g. Cable, DSL, Dial-up) with port/protocol filtering features enabled in a deny-by-default configuration for ingress traffic. Antivirus software (e.g. Symantec Antivirus) with current virus definitions and real-time scanning is also required and must be enabled. Firewall and Antivirus software is available at no cost to the requestor at https://infosec.navy.mil.
4. Managing the health and security of the non-U.S. Government computer is the requestor's responsibility. All security related configuration, patches and updates are required to be installed for the Operating System and any applications resident on the system.
5. All software installed on the home computer must be installed by the requestor after validating the source of the software is trusted. If unsure whether a vendor or software title can be trusted, the ONE-NET site IAM should be contacted. Installation of freeware / shareware is strongly discouraged. Warez, and Peer-to-Peer file sharing programs (E.G., Kazza, Morpheus, or Limewire) shall not be installed.
6. No unsecured external network connections such as wireless hubs or multiple networking/dial-in services shall be used while accessing OWA. No unmanaged remote access to the home computer is permitted. Use of secured wireless connections shall be compliant with DOD and Navy policy.
7. If emails are downloaded and stored, encrypt the files using 3DES or AES encryption. The use of Windows Encrypting File System (EFS) on Windows XP Pro SP1 (uses AES by default) for example, meets this requirement.
8. Ensure physical security of the system even if the OWA accessed/obtained contents are encrypted on the drive.
9. The requestor is not authorized to utilize OWA related systems for un-approved application connections.
10. Peripherals other than a standard cabled network interface device, a directly connected printer, keyboard and mouse shall not be connected to the privately owned computer while accessing OWA.
11. Any emails or the attachments it contains are not permitted to be stored on the non-U.S. Government owned machine if it is Sensitive information. Consult with the sender of the email or the command IAM if you are unsure if the data is Sensitive. Sensitive data such as Privacy Act Data must be handled in accordance with its data classification rules for handling. If it is believed a downloaded attachment contains Sensitive data, step 1 in Part IIa above shall be followed and in addition "Delete Files" on the General tab of the Internet Explorer properties page shall be selected to remove the file from the temporary files folder.

Requestor Initials __________

12. In the event of a classified spillage on a privately owned computer, it and all removable media (includes any media connected to the system during or after completing OWA use) shall be surrendered to government/military authorities. In certain cases, efforts to sanitize the system or removable media (hard disks, memory cards, stick memory, etc) may require physical destruction and the owner will not be compensated for the loss. The owner of the system or removable media (includes the owner of resident data) will also not be compensated for the lack of access to the privately owned computer during the period of time it takes to remediate the system or removable media from the effects of the spillage including the loss of any resident data. By using OWA, the user accepts all risks associated with remnance removal on the affected system and media, including the loss of the non-volatile memory device(s) and all data stored on them.

Requestor Initials __________

PART IId - USER AGREEMENT (Consent to Monitor)

19. OWA is provided through a Department of Defense Computer System. This computer system, including all related equipment, networks, and network devices (specifically including internet access), are provided only for authorized U.S. Government use. DOD computer systems may be monitored for all lawful purposes, including to ensure their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DOD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored.

Use of this DOD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

Requestor Initials __________

PART III - ***By signing below you signify your understanding and agreement to the terms and conditions listed above. You also affirm that the information you have provided is accurate and complete information to the best of your knowledge.***

20a. USER SIGNATURE	20b. DATE *(YYYYMMDD)*

NAME (*Last, First, Middle Initial*)	DATE *(YYYYMMDD)*	SSN *(Last 4)* or ID #

PART IV - ENDORSEMENT OF ACCESS BY COMMANDING OFFICER

21. JUSTIFICATION FOR ACCESS

22a. CLASSIFICATION OF OWA ACCESS REQUIRED: □ CLASSIFIED □ UNCLASSIFIED	22b. VERIFICATION OF NEED-TO-KNOW I certify that this user has need-to-know for data access for the OWA system classifications selected. □

23. ACCESS EXPIRATION DATE (*Contractors must additionally specify Company Name, Contract Number, Contract Expiration Date.*)

24a. COMMANDING OFFICER (CO) (*Print name*)	24b. CO EMAIL ADDRESS	24c. CO PHONE (*DSN or Commercial*)
24d. CO ORGANIZATION/DEPARTMENT	24e. COMMANDING OFFICER SIGNATURE	24f. DATE (*YYYYMMDD*)

PART V - ONE-NET IAM VALIDATATION OF SAAR / USER ACKNOWLEDGEMENT FORM ON FILE (*Must have been signed prior to 13 JUN 06*)

25a. SYSTEM AUTHORIZATION ACCESS REQUEST FOR ONE-NET REQUIREMENT □ User has a valid SAAR / User Acknowledgement Form on file	25b. DATE FILED *(YYYYMMDD)* ______________________

26a. VERIFIED BY *(ONE-NET IAM Print name)*	26b. ONE-NET IAM TELEPHONE NUMBER	26c. ONE-NET IAM SIGNATURE	26d. DATE (*YYYYMMDD*)

PART VI - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION

27a. DATE PROCESSED (*YYYYMMDD*)	27b. PROCESSED BY (*Print name*)	27c. PROCESSED BY (*Signature*)	27d. DATE (*YYYYMMDD*)

PART VII - DEACTIVATION OF OWA ACCESS BY AUTHORIZED STAFF

28a. DATE PROCESSED (*YYYYMMDD*)	28b. PROCESSED BY (*Print name*)	28c. PROCESSED BY (*Signature*)	28d. DATE (*YYYYMMDD*)

INSTRUCTIONS

The prescribing document is as issued by NETWARCOM for the use of OWA. Additional policies may apply.

(1) Type of request. Choose one: Initial, Modification, or Deactivation.

(2) ONE-NET User Logon Name(s). Provide requestor's existing UNCLASS and CLASS logon, if any.

PART I - Requestor Information. The following information is provided by the requestor when establishing, modifying, or deactivating their ONE-NET OWA account.

(3) Name. Print requestor's last name, first name, and middle inital.

(4) For U.S. Citizens, last 4 digits of Social Security Number. For those without an SSN, provide an ID number that identifies you to the U.S. DoD.

(5) Phone. Requestor's Defense Switching Network (DSN) phone number. If DSN is unavailable, provide a commercial phone number.

(6) Command UIC/PLA. Requestor's Command Unit Identification Code or Plain Language Address.

(7) Office Symbol/Department. The office symbol within the current organization (i.e. NNWC).

(8) Building Number/Room Number. Requestor's work space building number and room number.

(9) Official Mailing Address. Requestor's official business mailing address.

(10) Job Title and Grade/Rank. Requestor's job title and grade/rank. (Examples: Civilian - Systems Analyst, GS-14, Pay Clerk, GS-5; Military - COL, US Army, CMSgt, USAF; or Contractor - Database Administrator, CONT).

(11) Citizenship. US, Foreign National, or Other (provide Other country).

(12) Designation of Person. Choose one: Military, Civilian, Contractor, or Foreign National Indirect Hire.

(13) Parent Organization/Organization. Requestor's parent organization and organization.

(14) PCS/Departure Date. Requestor's permanent change of station or expected date of departure from site.

(15) Date. The date the Requestor signs the form. Format: 4 digit year, 2 digit month, 2 digit day (*YYYYMMDD*).

PART IIa - (16) User must initial this section with acknowledgement that the user is responsible for understanding and accountable for the risks associated with OWA use.

PART IIb - (17) User must initial this section with acknowledgement that the user is responsible for understanding and accountable for the terms and conditions for CLASSIFIED OWA use.

PART IIc - (18) User must initial this section with acknowledgement that the user is responsible for understanding and accountable for the terms and conditions for UCLASSIFIED OWA use as well as additional conditions for using a non-US government computer.

PART IId - (19) User must initial this section with acknowledgement that the user is responsible for understanding and accountable for the consent to monitor.

PART III - (20a) User Signature. User must sign the ONE-NET OWA UAF with the understanding that they are responsible and accountable for their password and access to OWA.

(20b) Date. The date the user signs the form. Format: 4 digit year, 2 digit month, 2 digit day (*YYYYMMDD*).

PART IV - Endorsement of Access by Commanding Officer. The information below requires the endorsement from the user's Supervisor or Government Sponsor.
(21) Justification for Access. A brief statement is required to justify establishment of user's access. Specify here if the user already has a ONE-NET user logon or requires a modification to current account.

(22a) Classification of OWA Access Required. Select CLASSIFIED, UNCLASSIFIED, or both.

(22b) Verification of Need-to-Know. Verify that the user requires access as requested.

(23) Access Expiration Date. Normally PCS, departure date, or other known access expiration date. Additionally, contractors must provide Company Name, Contract Number, and Contract Expiration Date.

(24a) Commanding Officer (CO). Commanding Officer or supervisor with by direction signature authority name is printed here to indicate that the above information has been verified and that access is required.

(24b) Commanding Officer's Signature. Commanding Officer or supervisor with by direction signature authority signature is required.

(24c) Date. The date the Commanding Officer or supervisor with by direction signature authority signs the form. Format: 4 digit year, 2 digit month, 2 digit day (*YYYYMMDD*).

(24d) CO Organization/Department.Commanding Officer or supervisor with by direction signature authority organization and department.

(24e) CO Email Address. Commanding Officer or supervisor with by direction signature authority official email address.

(24f) CO Phone. Commanding Officer or supervisor with by direction signature authority DSN phone number. If DSN is unavailable, provide a commercial phone number.

PART V - ONE-NET Information Assurance Manager (IAM) validation of SAAR/User Acknowledgement Form on file. This must have been signed prior to 13 JUN 06.
(25a) System Authorization Access Request for ONE-NET Requirement. Mark this section if the user has a valid User Acknowledgement Form on file.

(25b) Date Filed. If (25a) was marked, provide date that the User Acknowledgement Form was filed. Format: 4 digit year, 2 digit month, 2 digit day (*YYYYMMDD*).

(26a) Verified By ONE-NET IAM. Print ONE-NET IAM's name or Appointee.

(26b) ONE-NET IAM Telephone Number. ONE-NET IAM or Appointee's DSN phone number. If DSN is unavailable, provide a commercial phone number.

(26c) ONE-NET IAM Signature. ONE-NET IAM's signature is required for approving account creation, modification, or deactivation for OWA.

(26d) Date. The date the ONE-NET IAM signs the form. Format: 4 digit year, 2 digit month, 2 digit day (*YYYYMMDD*).

PART VI - Completion by authorized staff preparing account information.

(27a) Date Processed. The date the user's request is processed. Format: 4 digit year, 2 digit month, 2 digit day (*YYYYMMDD*).

(27b) Processed By (Print name). Print name of authorized staff who processed user's request.

(27c) Processed by (Signature). Signature of authorized staff who processed user's request.

(27d) Date. The date the authorized staff signed the form.

PART VII - Deactivation of OWA access by authorized staff.

(28a) Date Processed. The date the user's account is deactivated. Format: 4 digit year, 2 digit month, 2 digit day (YYYYMMDD).

(28b) Processed By (Print name). Print name of authorized staff who deactivated user's OWA account.

(28c) Processed by (Signature). Signature of authorized staff who deactivated user's OWA account.

(28d) Date. The date the authorized staff signed the form.

DISPOSITION OF FORM

TRANSMISSION: Form may be faxed, mailed or scanned and sent electronically.

CLASSIFICATION: When completed, this form becomes "FOR OFFICIAL USE ONLY" and must be protected as such.

FILING: This form will be maintained by the ONE-NET IAM for three years after termination of the requestor's OWA access.