



ONE-NET ACCOUNT SUBMISSION PACKAGE CHECKLIST

ONE-NET SUBMISSION PACKAGE CHECKLIST

Do not submit the Accounts package without having the following items:

| | |
|--------------------------|---|
| <input type="checkbox"/> | <u>SAAR-N</u> - Completely filled in form (Blocks 1-32, 33-37(SIPR ONLY) and ALL signatures |
| <input type="checkbox"/> | <u>User Validation Form (UVF)</u> - ALL sections completely filled in. |
| <input type="checkbox"/> | <u>Keyboard Video Mouse (KVM) User Agreement</u> |
| <input type="checkbox"/> | <u>DOD IAA Certificate v8.0</u> (http://iase.disa.mil/eta/iaav8/iaav8/index.htm) |

Please Submit the complete Accounts Package (SAAR, UVF, KVM, IAA v8.0) to ServiceDesk.Accounts@me.navy.mil (GAL → Service Desk Middle East Accounts)

USER VALIDATION FORM (NIPRNET & SIPRNET)

Complete all requested information and maintain a copy for your records

PRIVACY ACT STATEMENT

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; Joint Ethics Regulation; and E.O. 9397.

Principal Purpose: For use in conjunction with OPNAV 5239/14, System Authorization and Access Request-Navy, to ensure that all personnel using Department of the Navy (DoN) owned or leased automated data processing equipment, information systems and information data, hereafter called the OCONUS Navy Enterprise Network (ONE-Net) are correctly identified and authenticated. Collection of the SSN and DNI information and other personal identifiers are used to ensure positive identification of the user who requests services from the Theater Network Operations and Security Center (TNOSC), Bahrain and its Local Network Service Centers (LNSCs). Records may be maintained in both electronic and/or paper form.

Disclosure: Voluntary; however, failure to disclose information could result in delayed or denial of service from ONE-NET

Last 4 of SSN or last 5 of DNI:

Last Name, First Name, Middle Initial:

Base Location:

PRD (Rotation Date):

PIN Code (**4 numbers ONLY** - strongly recommend **NOT** using last 4 of SSN):

Do NOT use sequential numbers (i.e., 0000, 1111, 0123, 4567,6789, etc)

Do NOT use Common Access Card (CAC) Pin number

Secret Word (**6 - 10 letters ONLY** -- NO numbers or special characters (#%):

Do NOT use any part of your full name, rank or current location

Do not submit the SAAR-N package without having the following items:

- Completely filled in SAAR-N form (Blocks 1-32, 33-37(SIPR ONLY) and ALL signatures
- ALL sections completely filled in on the User Validation Form
- DOD IAA Certificate v8.0 (<http://iase.disa.mil/eta/iaav8/iaav8/index.htm>)
- Keyboard Video Mouse (KVM) User Agreement

Please Submit the complete SAAR-N Package (SAAR, UVF, KVM, IAA CERT v8.0) to ServiceDesk.Accounts@me.navy.mil (Listed in the GAL as Service Desk Middle East Accounts)

| | |
|--|---|
| 25. NAME (Last, First, Middle Initial) | 25a. SOCIAL SECURITY NUMBER (LAST FOUR) |
| <p>26. USER AGREEMENT - STANDARD MANDATORY NOTICE AND CONSENT PROVISION</p> <p>By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:</p> <ul style="list-style-type: none"> - You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government-authorized use only. - You consent to the following conditions: <ul style="list-style-type: none"> o The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE) and counterintelligence (CI) investigations. o At any time, the U.S. Government may inspect and seize data stored on this information system. o Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose. o This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy. o Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below: <ul style="list-style-type: none"> - Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality. - The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies. - Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality. - Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy. - A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality. - These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected. o In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information. o All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement. | |
| 27. USER SIGNATURE | 28. DATE (YYYYMMDD) |

| | |
|--|---|
| 29. NAME (Last, First, Middle Initial) | 29a. SOCIAL SECURITY NUMBER (LAST FOUR) |
|--|---|

30. USER RESPONSIBILITIES

I understand that to ensure the integrity, safety and security of Navy IT resources, when using those resources, I shall:

- Safeguard information and information systems from unauthorized or inadvertent modification, disclosure, destruction, or use.
- Protect Controlled Unclassified Information (CUI) and classified information to prevent unauthorized access, compromise, tampering, or exploitation of the information.
- Protect passwords for systems requiring logon authentication and safeguard passwords at the sensitivity level of the system for classified systems and at the confidentiality level for unclassified systems. Passwords will be classified at the highest level of information processed on that system.
- Virus check all information, programs, and other files prior to uploading onto any Navy IT resource.
- Report all security incidents immediately in accordance with local procedures and CJCSM 6510.01 (series).
- Access only that data, control information, software, hardware, and firmware for which I am authorized access and have a need-to-know, and assume only those roles and privileges for which I am authorized.

I further understand that, when using Navy IT resources, I shall not:

- Access commercial web-based e-mail (e.g. HOTMAIL, YAHOO!, AOL, etc.)
- Auto-forward official e-mail to a commercial e-mail account.
- Bypass, strain, or test IA mechanisms (e.g., Firewalls, content filters, anti-virus programs, etc.). If IA mechanisms must be bypassed, I shall coordinate the procedure and receive written approval from the Local IA Authority (CO or OIC).
- Introduce or use unauthorized software, firmware, or hardware on any Navy IT resource.
- Relocate or change equipment or the network connectivity of equipment without authorization from my Local IA Authority.
- Use personally owned hardware, software, shareware, or public domain software without authorization from the Local IA Authority.
- Upload executable files (e.g., .exe, .com, .vbs, or .bat) onto Navy IT resources without the approval of the Local IA Authority.
- Participate in or contribute to any activity resulting in a disruption or denial of service.
- Write, code, compile, store, transmit, transfer, or introduce malicious software, programs, or code.
- Put Navy IT resources to uses that would reflect adversely on the Navy (such as uses involving pornography; chain letters; unofficial advertising, soliciting or selling except on authorized bulletin boards established for such use; violation of statute or regulation; inappropriately handled classified information; and other uses that are incompatible with public service).

| | |
|--------------------|----------|
| 31. USER SIGNATURE | 32. DATE |
|--------------------|----------|

PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION

| | | | |
|------------------------------|---------------------------------------|---|---------------------|
| 33. TYPE OF INVESTIGATION | | 33a. DATE OF INVESTIGATION (YYYYMMDD) | |
| 33b. CLEARANCE LEVEL | | 33c. IT LEVEL DESIGNATION <input type="checkbox"/> LEVEL 1 <input type="checkbox"/> LEVEL 2 <input type="checkbox"/> LEVEL 3 | |
| 34. VERIFIED BY (Print name) | 35. SECURITY MANAGER TELEPHONE NUMBER | 36. SECURITY MANAGER SIGNATURE | 37. DATE (YYYYMMDD) |

PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION

| | | |
|---------------------------------|---|----------------------|
| 38. TITLE: | 38a. SYSTEM | 38b. ACCOUNT CODE |
| | 38c. DOMAIN | |
| | 38d. SERVER | |
| | 38e. APPLICATION | |
| | 38f. DIRECTORIES | |
| | 38g. FILES | |
| | 38h. DATASETS | |
| 39. DATE PROCESSED (YYYYMMDD) | 39b. PROCESSED BY (Print name and sign) | 39c. DATE (YYYYMMDD) |
| 40. DATE REVALIDATED (YYYYMMDD) | 40a. REVALIDATED (Print name and sign) | 40b. DATE (YYYYMMDD) |

INSTRUCTIONS

A. PART I: The following information is provided by the user when establishing or modifying their USER ID.

- (1) Name. The last name, first name, and middle initial of the user.
- (2) Social Security Number. The last four numbers in the social security number of the user.
- (3) Organization. The user's current organization (i.e., USS xx, DoD, and government agency or commercial firm).
- (4) Office Symbol/Department. The office symbol within the current organization (i.e., SDI).
- (5) Telephone Number/DSN. The Defense Switching Network (DSN) and commercial phone number of the user.
- (6) Official E-mail Address. The user's official e-mail address.
- (7) Job Title/Grade/Rank. The civilian job title (i.e., Systems Analyst, YA-02, military rank (CAPT, United States Navy) or "CONT" if user is a contractor.
- (8) Official Mailing Address. The user's official mailing address.
- (9) Citizenship (U.S., Foreign National or Other).
- (10) Designation of Person (Military, Civilian, Contractor).
- (11) IA Training and Awareness Certification Requirements. User must indicate if he/she has completed the Annual Information Awareness Training and the date.
- (12) User's Signature. User must sign the OPNAV 5239/14 with the understanding that they are responsible and accountable for their password and access to the system(s).
- (13) Date. The date the user signs the form.

B. PART II: The information below requires the endorsement from the user's Supervisor or the Government Sponsor.

- (14) Justification for Access. A brief statement is required to justify establishment of an initial USER ID. Provide appropriate information if the USER ID or access to the current USER ID is modified.
- (15) Type of Access Required: Place an "X" in the appropriate box. (Authorized - Individual with normal access. Privileged - Those with privilege to amend or change system configuration, parameters or settings.)
- (16) User Requires Access To. Place an "X" in the appropriate box. Specify category.
- (17) Verification of Need to Know. To verify that the user requires access as requested.
- (17a) Expiration Date for Access. The user must specify expiration date if less than 1 year.
- (18) Supervisor's Name (Print Name). The supervisor or representative prints his/her name to indicate that the above information has been verified and that access is required.
- (18a) Supervisor's Signature. Supervisor's signature is required by the endorser or his/her representative.
- (18b) Date. Date supervisor signs the form.
- (19) Supervisor's Organization/Department. Supervisor's organization and department.
- (19a) E-mail Address. Supervisor's e-mail address.
- (19b) Phone Number. Supervisor's telephone number.
- (20) Signature of Information Owner/OPR. Signature of the functional appointee responsible for approving access to the system being requested.
- (20a) Phone Number. Functional appointee telephone number.
- (20b) Date. The date the functional appointee signs the OPNAV 5239/14.

- (21) Signature of Information Assurance Officer (IAO) or Appointee. Signature of the IAO or Appointee of the office responsible for approving access to the system being requested.
- (22) Organization/Department. IAO's organization and department.
- (23) Phone Number. IAO's telephone number.
- (24) Date. The date IAO signs the OPNAV 5239/14.
- (25) Name. The last name, first name, and middle initial of the user.
- (25a) Social Security Number. The last four numbers in the user's social security number.
- (26) Standard Mandatory Notice and Consent Provision. This item is in accordance with DoD memo dtd May 9, 2008 (Policy on Use of DoD Information Systems - Standard Consent Banner and User Agreement).
- (27) User Signature. User signs.
- (28) Date. Date signed.
- (29) Name. The last name, first, name and middle initial of the user.
- (29a) Social Security Number. The last four numbers in the social security number of the user.
- (30) User Responsibilities
- (31) User Signature. Member signs.
- (32) Date. Date signed.

C. PART III: Certification of Background Investigation or Clearance.

- (33) Type of Investigation. The user's last type of background investigation (i.e., NAC, NACI or SSBI).
- (33a) Date of Investigation. Date of last investigation.
- (33b) Clearance Level. The user's current security clearance level (Secret or Top Secret).
- (33c) IT Level Designation. The user's IT designation (Level I, Level II or Level III).
- (34) Verified By. The Security Manager or representative prints his/her name to indicate that the above clearance and investigation information has been verified.
- (35) Security Manager Telephone Number. The telephone number of the Security Manager or his/her representative.
- (36) Security Manager Signature. The Security Manager or his/her representative indicates that the above clearance and investigation information has been verified.
- (37) Date. The date that the form was signed by the Security Manager or his/her representative.

D. PART IV: This information is site specific and can be customized by either the functional activity or the customer with approval from NAVNETWARCOM. This information will specifically identify the access required by the user.

(38 - 40b). Fill in appropriate information.

E. DISPOSITION OF FORM:

TRANSMISSION: Form may be electronically transmitted, faxed or mailed. If transmitted electronically, the email must be digitally signed and encrypted.

FILING: Retention of this form shall be in accordance with SECNAV M5210-1, Records Management Manual (Section 5230.2 applies).

UNCLASSIFIED/FOUO

KVM (Keyboard Video Mouse) USER AGREEMENT

PRIVACY ACT STATEMENT

AUTHORITY: 5 U.S.C. 301; 10 U.S.C. 131. PRINCIPAL PURPOSE(S): Identifies the user of the KVM device as receiving usage and security awareness training governing use of the device and agreeing to use the device in accordance with security policies. The information is used for inventory control of the device and to verify compliance with DoD requirements regarding accountability security requirements IAW Sharing Peripherals Across the Network Security Technical Implementation Guide (SPAN STIG) 3.1
ROUTINE USE(S): None.
DISCLOSURE: Voluntary; however, failure to provide the requested information will result in denial to operate or use of the KVM.

PART I - PERSONAL INFORMATION

| | | |
|--------------------|-----------------|--------------------------|
| 1. LAST NAME | 2. FIRST NAME | 3. MIDDLE INITIAL |
| 4. RANK/RATE | 5. ORGANIZATION | 6. DEPARTMENT/DIVISION |
| 7. BUILDING NUMBER | 8. ROOM NUMBER | 9. WORK TELEPHONE NUMBER |
| 10. E-MAIL ADDRESS | | |

PART II - USER AGREEMENT – Standard Mandatory and Consent Provision

User Will:

- Ensure that the switches are approved before installing
- Ensure that the systems are installed correctly and meet all TEMPEST standards
- Ensure the desktop banners, backgrounds, and screen locks have the proper classification banner
- Protect the system and KVM in your area
- Report any spillage of classified information to your IAO or the IAM
- Safeguard and report any unexpected or unrecognized computer output, including both displayed or printed products
- Use different passwords on each system connected through a KVM
- Ensure that the classification level is displayed by each systems screen lock and that the password is required to regain entry to the system
- Ensure that the systems screen lock is invoked if the system is left unattended or if there is a 15-minute period of inactivity for each system
- Be responsible for marking/labeling magnetic media

Administrative Procedures: Users are required to follow the procedures below when using KVM switches:

1. Logon onto an IS.
 - a. Identify the classification of the IS currently selected.
 - b. Use the login and passwords appropriate for that IS.
 - c. Verify the classification of the present IS by checking the classification label/banner.
 - d. Begin processing.
2. Switching between ISs.
 - a. Screen lock the IS you are currently using if the IS supports this capability.
 - b. Select the desired IS with the switch.
 - c. Enter the user identifier and password to deactivate the screen lock on the newly selected IS.
 - d. Verify the classification of the present IS by checking the classification label/banner.
 - e. Begin processing.

Physical Security Controls:

KVM switches are normally unclassified devices; however, it must be protected in a manner suitable for the IS with the highest classification to which it is connected. For example, if the switch is connected to a classified system and an unclassified system, then it will be protected in the same manner as the classified system. Physical access to the KVM switch must also be restricted to individuals that are allowed physical access to all ISs attached to the system.

Labels:

All IS components must be labeled, including all switch positions. They must be clearly marked with the appropriate classification labels.

Desktop Backgrounds:

To avoid inadvertent compromises, systems joined by multi-position switches will utilize desktop backgrounds that display classification banners at the top or bottom. The classification banner will state the overall classification of the system in large bold type, and the banner background will be in a solid color that matches the classification (Secret - red, Confidential - blue, Unclassified - green).

When systems have a similar classification level, but require separation for releasability or other constraints, use of unique colors for the different systems is permissible.

Screen Locks:

Screen lock applications must display the highest classification of the system on which the system is currently logged into and shall implement a lockout feature to re-authenticate the user.

Smart Keys:

Systems using KVM switches must not employ "smart" or memory enhanced/data retaining keyboards, monitors or mice. These types of interfaces provide memory retention that creates a risk of data transfer between systems of different classifications. This includes keyboards with smart card readers, Universal Serial Bus (USB) ports, and removable media drives.

Hot Key Capability:

If the switch has configurable features, the configuration must be protected from modification by the user with a DOD compliant password.

Switches featuring the ability to automatically toggle between Information Systems (IS) must have this feature disabled. The only "hot key" feature permitted to be enabled is the menu feature that allows the user to select the IS to be used from a displayed menu.

Scanning Capability:

Switches with the ability to automatically scan and switch to different CPUs are prohibited.

Wireless or Infrared Technology:

Systems using KVM switches must not use keyboards or mice with wireless or infrared technology.

Connectors:

The use of switches to share peripherals other than the keyboard, video/monitor, and mouse by connecting peripherals to ISs of different classification levels is prohibited. All switches that are attached to ISs of different classifications will have this feature disabled. Regardless of whether it can be disabled, no peripheral devices other than the keyboard, video/monitor, or mouse will be connected to the KVM switch.

Connectors used for this feature will be blocked with tamper resistant seals. Additionally, all unused connectors for ISs will be blocked with tamper resistant seals. All cable connections will be marked with tamper resistant seals that allow visual confirmation that the configuration of the cable has not been modified.

Unique Password:

At a minimum, users must ensure that they use different/unique passwords for each system connected through a switch. System administrators should employ different logon USERIDs to help users further distinguish between the systems.

Training:

Periodic training is required to ensure that users are trained and in compliance with the requirements associated with the introduction and use of KVM switches.

FOR REPORTING PROBLEMS OR TO ASK QUESTIONS, CONTACT NCTS-ME Enterprise Service Desk (ESD): 439-6287

By signing this document, I acknowledge that I have read and understood my duties and responsibilities in relation to the use, operation, and information security requirements of the KVM switch.

12. SIGNATURE OF USER

13. DATE SIGNED (YYYYMMDD)

UNCLASSIFIED/FOUO



ONE-NET ENTERPRISE SERVICE DESK ACCOUNTS SETUP QUICK GUIDE

Road-Map to creating a ONE-NET Account

Step 1 – Download, Completely fill out and Email the ONE-NET Account Submission Package (SAAR-N Form, User Verification Form, KVM, IAA Cert V8.0) to Servicedesk.Accounts@me.navy.mil (In Global, Service Desk Middle East Accounts)

- Download and print the One-Net Account Submission Package from:
 - <https://intranet.me.navy.mil/> (Click on TNOSC-N8 -> One-Net Docs)
 - http://www.public.navy.mil/USFF/NCTSBHAIRAIN/OCONUS_TNOSC/Pages/ONE-Net_Documents.aspx
- Submission package should include: SAAR-N, User Validation Form, KVM and IAA Cert V8.0
- IAA Cert V8.0 can be found at <http://iase.disa.mil/eta/iaav8/iaav8/index.htm>
- Coordinate with your commands IA or N6 departments on correctly filling out and submitting the package.
- If a problem exists with your submission, the accounts department will contact you to correct the issue.

Step 2 – Account Package will be processed within 48-72 hours.

- Accounts are typically created within 48-72 hours from the time of submission.
- To verify if your account has been created, you can
 - Have a colleague check the GAL to see if your name is listed
 - Call the Enterprise Service Desk Accounts department x6004
 - Call the Enterprise Service Desk Call Center at x6287

Step 3 – Perform the First-Time Login using Username and Default Password.

- Username will be either First.Last (Mil), First.Last.ctr (CTR), First.Last.CC (Foreign National, CC is the specific country code)
- Default password is last4SSN@Me.Bahrain – Note this is case sensitive. If password does not work, call the enterprise service desk and they can reset your password over the phone using your User Verification Form (UVF)
- Domain is DS.
- Once you enter the default and press enter, it will prompt you to change your password: password should be 14 characters long, including (2 Upper, 2 lower, 2 Numbers, 2 special Characters)

Step 4 – CLO – Setting up your CAC for login (NIPR Users).

- Once you login the first time with your username and password, you should receive a prompt to enter your CAC card to be configured so you can login with your CAC.

Step 5 – Setup Email

- Open MS Outlook and it will prompt you to setup your email
- Select Microsoft Exchange Server
- Enter exchange server – UMEBAEX02 (NIPR) or MEBAEX02 (SIPR)
- Enter username and click check name. If it resolves, then you entered correctly.
- Click finish and you should be connected to your email.

Step 6 – Remedy profile Setup (Used for verification and over-the-phone password resets and account unlocks)

- Go to <https://servicedesk.me.navy.mil/>
- Select Email Cert
- Click on Requester Console
- Click on Update my info
- Enter pin and secret word and click save.



ONE-NET ENTERPRISE SERVICE DESK ACCOUNTS SETUP QUICK GUIDE

| Enterprise Service Desk Contact Info | |
|--------------------------------------|--|
| ESD Call Center (HelpDesk) | COMM - 011.973.1785.NCTS(6287) or DSN - 439.NCTS(6287) |
| ESD Main Email | ServiceDesk.Bahrain@me.navy.mil (In Global, Service Desk Middle East) |
| ESD Accounts Email | ServiceDesk.Accounts@me.navy.mil (In Global, Service Desk Middle East Accounts) |

| What do I get as a ONE-NET User? |
|---|
| <p>Services and support are provided for both NIPRNET and SIPRNET:</p> <ul style="list-style-type: none"> a. Email b. File Sharing c. Print d. Network e. Desktop hardware and standard software support f. Information assurance/security g. Remote connectivity (NIPRNET broadband, NIPRNET dial-in, NIPRNET OWA, limited SIPRNET dial-in, and SIPRNET OWA) h. Directory services – an OCONUS GAL |

| Capability | Service | Baseline |
|-----------------------------------|-------------------------------|--|
| Enterprise Service Desk/Help Desk | | |
| | Enterprise Service Desk | 24 x 7 availability - 439-NCTS (6287) |
| | New Accounts | 24-48 hours |
| E-mail | | |
| | NIPR Storage | 100 MB |
| | SIPR Storage | 100 MB |
| | e-mail address | firstname.lastname@me.navy.mil (MIL) firstname.lastname.ctr@me.navy.mil (CTR) firstname.lastname@me.navy.mil (MIL) |
| | Incoming attachment limit | 30 MB |
| | Outgoing attachment limit | 10 MB |
| | Current address forwarding | 30 days for regular users, 90 days for VIPs |
| Shared Storage | | |
| | Personal Home Drive | 850 MB per user |
| | Command Share Drive | 150 MB per user, per Command |
| Remote Access | | |
| | Virtual Private Network (VPN) | To remote into the network, based on Command approval |
| | Outlook Web Access (OWA) | To remotely access e-mail, with Command approval |

| ONE-NET Important Links | |
|----------------------------|---|
| Intranet Navy Site | https://intranet.me.navy.mil |
| Public Navy Site | http://www.public.navy.mil/usff/nctsbahrain/ |
| Remedy Trouble Ticket Site | https://servicedesk.me.navy.mil/ |