DEPARTMENT OF THE NAVY
COMMANDER NAVY RESERVE FORCE
1915 FORRESTAL DRIVE
NORFOLK VA 23551-4615

COMNAVRESFORINST 5300.5D
N6
1 Oct 2024

COMNAVRESFOR INSTRUCTION 5300.5D

From: Commander, Navy Reserve Force

Subj: INFORMATION TECHNOLOGY AND NAVY MARINE CORPS INTRANET GUIDANCE

Ref: (a) CIO memo of 19 Aug 19 MFD Guidance
(b) DoD 5500.07-R, Joint Ethics Regulation, November 2011
(c) SECNAV 192027Z Aug 10
(d) SECNAV 192031Z Aug 10
(e) SECNAVINST 5239.3B
(f) SECNAVINST 5210.8E
(g) DON CIO 032009Z Oct 08 (h) 44 U.S.C. § 3541
(h) SECNAV M-5510.30, Department of the Navy Personnel Security Program
(i) SECNAV M-5210.1, Rev. 1, Records Management Manual
(j) COMNAVNETWARCOM ltr 5239 Ser ODAA/1001 of 9 May 11
(k) DON CIO 161108Z Jul 05
(l) DoD Instruction 8500.2 of 6 February 03
(m) DDCIO (N) memorandum of 17 Sep 13
(n) DSECDEF memo 15 Jan 18, Conducting Official Business on Electronic Messaging Accounts
(o) CNO Washington DC 121935Z Mar 12 (NAVADMIN 084/12) Router Network
(p) CMS-1 Department of the Navy (DON) COMSEC Policy and Procedures Manual
(q) SECNAV M-5510.36 Department of the Navy Information Security Program
(r) Acceptable Use of Department of the Navy (DON) Information Technology (IT)
(s) Memo 12 February 2016
(t) DoD Registration Practice Statement
(u) SECNAV M-5239.2
(v) DoD Directive 8140
(w) CNO Washington DC 201202Z Sep 17
(x) COMNAVRESFORINST 5239.3A
(y) NAVADMIN 148/20
(z) SECNAVINST 1543.2

Encl: (1) Administrative Information Technology Procedures for the Navy Reserve Force

1. Purpose. The purpose of this instruction is to promulgate guidance for Navy Reserve Information Technology (IT) usage to meet clamancy-wide requirements. These requirements maximize efficiency and cost effectiveness for Enterprise Architecture (EA), Information Assurance (IA), Cybersecurity, Security, Management, Distribution, and Administration and User Responsibilities, per references (a) through (z), within a limited Navy Marine Corps Intranet (NMCI) and Next Generation (NGEN) budget. This instruction is a complete revision and should be reviewed in its entirety.

2. Cancellation. COMNAVRESFORINST 5300.5C

3. Scope. Enclosure(1) provides policy for the administration of the Navy Reserve Force's IT investments and IT services portfolio. Due to the rapid pace and evolving nature of IT and related

systems, in addition to this document, users will reference the Commander, Navy Reserve Forces Command (COMNAVRESFORCOM) Information Technology N6 SharePoint page for further clarification, guidance, and updates to policy.

4. Records Management. Records created as a result of this instruction, regardless of media and format, must be managed per Secretary of the Navy Manual 5210.1 of September 2019.

5. Review and Effective Date. Review and Effective Date. Per OPNAVINST 5215.17A, COMNAVRESFORCOM N6 will review this instruction annually around the anniversary of its issuance date to ensure applicability, currency, and consistency with Federal, Department of Defense, Secretary of the Navy, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will be in effect for 10 years, unless revised or cancelled in the interim, and will be reissued by the 10-year anniversary date if it is still required, unless it meets one of the exceptions in OPNAVINST 5215.17A, paragraph 9. Otherwise, if the instruction is no longer required, it will be processed for cancellation as soon as the need for cancellation is known following the guidance in OPNAV Manual 5215.1 of May 2016.

M. J. STEFFEN
Deputy Commander

Releasability and distribution:
This instruction is cleared for public release and is available electronically only via COMNAVRESFOR Web site at https://www.navyreserve.navy.mil/Resources/Official-RESFOR-Guidance/Instructions/

ADMINISTRATIVE INFORMATION TECHNOLOGY PROCEDURES FOR THE NAVY RESERVE FORCE

Table of Contents

CHAPTER 1
NAVY MARINE CORPS INTRANET (NMCI) AND NETWORK SERVICES

1. NMCI Account Management

a. Active NMCI unclassified accounts are required for all service members of the Navy Reserve, including Training and Administration of the Reserves (TAR), Selected Reserve (SELRES), Volunteer Training Unit (VTU) members and all government civilian employees under the responsibility of Commander, Navy Reserve Force Command (COMNAVRESFORCOM). Contractors who are under contract with COMNAVRESFORCOM or any of its subordinate commands might be obligated to have these accounts.

b. NMCI email accounts will be created, processed and maintained at each services member's perspective echelon level command (i.e., echelon III, IV, and V). Individuals holding dual accounts (e.g., SELRES and a government civilian account) are required to utilize the account associated with the specific role from which they are sending an email. Every account profile will be created using the NMCI Enterprise Tool (NET). This will enable COMNAVRESFOR to consistently track the precise count of accounts allocated to COMNAVRESFOR at any given moment.

c. NMCI accounts will be deactivated upon the death, retirement or separation of a service member, civilian employee, or contractor. The command's Assistant Customer Technical Representative (ACTR) can opt temporary suspension or permanent deactivation. The Customer Technical Representative (CTR) may temporarily suspend an account if the service member intends to join the Navy in another capacity (TAR to SELRES or contractor, etc.). The account should be permanently deactivated if the member has not transferred after the 90-day period has expired. Shared or group mailboxes are not authorized unless specifically authorized in writing by COMNAVRESFOR Cyber Security (N64). Shared mailboxes do not support encryption of data e-mail. In this situation, non-repudiation is not inherently obvious for a specific service member, employee, or contractor.

d. Reactivation of the existing account is required for members who are transferring from a non-NMCI command or returning to a command with NMCI access. It's important to refrain from creating new accounts when an account is already present in the NMCI active directory.

e. Individuals holding NMCI accounts must log in at specified intervals, as established by Commander, Naval Network Warfare Command (COMNAVNETWARCOM), to prevent their accounts from being disabled or removed. It's important to note that the login requirements differ between the Active Component (AC) and Reserve Component (RC), which includes both SELRES and TAR.

(1) AC personnel accounts on the Non-Classified Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET) are controlled by the Active Organizational Unit (OU) which is deactivated following 30 days of inactivity, and subsequently removed after 45 days of dormancy (which is 15 days after disablement). This policy applies to all military, civilian, and contractor personnel.

(2) RC personnel accounts on the NIPRNET and SIPRNET are controlled by the Reserve OU which is deactivated after 60 days of inactivity and subsequently removed after 180 days of dormancy. This policy is applicable to all military, civilian, and contractor personnel who are under the jurisdiction of COMNAVRESFOR.

(3) Note, this policy is subject to potential changes in accordance with COMNAVNETWARCOM directives. For the latest policy updates, it is recommended to contact COMNAVRESFOR Information Technology (N6). To prevent the deletion of accounts for members who are mobilizing, units should initiate a request for a deployed status through COMNAVNETWARCOM's access management team. This can be done via their Information Systems Security Manager (ISSM) or Information Systems Security Officer (ISSO) using the provided template. Units are responsible for requesting the removal of members from the deployment status upon their return. Example email for requesting deployed status:

To: NNWC_ACCESS.MGMT@us.navy.mil
Subject: Deployed user ICO <username goes here>
Please place the below Sailor's account in the "Deployed Users" queue to stop the account from being disabled and/or deleted.
Name:
NIPRNET or SIPRNET User ID:
Reason:
Return Date:

2. Account Definitions:

a. Active Account: This type of account grants the member access to the NMCI network, email services, and personal storage space, including OneDrive.

b. Deactivated Account: This status indicates the end of service for an NMCI Account. Deactivation takes place when all NMCI services are terminated. The account will be relocated from the local command's OU structure, resulting in streamlined attributes within the digital identity and a flat name space. Any associated data will be compacted and transferred to a permanent data storage facility. It's important to note that accounts of members transferring between commands under NMCI service should not be deactivated.

c. Disabled Account: This type of account is inaccessible, and all email communication sent to it is rejected. The disabled account status is managed by the ISSM to prevent logins and effectively disable the account.

d. Reactivated Account: A reactivated account is one that has been restored to an active state using its previously stored digital identity.

3. SIPRNET Accounts and Tokens.

a. Within the Navy Reserve Force, the terms "SIPRNET account" and "SIPRNET token" are used interchangeably by Navy Reserve Force service members, government civilians, and contractors. A SIPRNET account refers to the approved, allocated, and authorized permission for a Total Force member to utilize electronic or networked SIPR media. On the other hand, a SIPRNET token is the tangible hardware item, typically an access card, which serves as a means of authentication to access an account. Refer to APPENDIX C "Process for Command Trusted Agents (TA) to stand up or request SIPR Account/Tokens" for further information/guidance.

b. Periodicity.

(1) SIPR Account: After 60 days of dormancy, SIPR accounts are disabled; following 180 days of dormancy, they are permanently deleted.

(2) SIPR Token: SIPR tokens do not have an inherent expiration date, but the certificates stored on the token are valid for three years. After this three-year period, the token's certificates must be refreshed to maintain functionality.

c. Not all Navy Reserve total force members are eligible for SIPR access per COMNAVRESFOR guidance. COMNAVRESFOR does not mandate that every Navy Reserve member possesses a SIPRNET account. However, if a member is identified by their chain of command as requiring access due to a legitimate need to know and possessing the necessary security clearance, a request for a NMCI SIPRNET account may be initiated.

(1) To make such a request, submit a completed System Authorization Access Request-Navy (SAAR-N) form and a DD-2842 (AUG-2009) form. For proof of identity, a Common Access Card (CAC) must be provided. The creation of the account, generated through a Move, Add, and Change (MAC) submission, generally takes between one to five business days by NMCI, provided the request is accurate and complete.

(2) This process is managed by the echelon 5 Navy Reserve Activity (NRA), such as Navy Reserve Center (NAVRESCEN) or a Squadron. Once NRA's NMCI representative (such as CTR, Deputy Customer Technical Representatives (DCTR), ACTR) receives the account creation notification email from NMCI, the Total Force member has a 60-day window to meet in person (physical presence is mandatory) with a Local Registration Authority (LRA) or Trusted Agent (TA) to obtain a token associated with their new account. Failure to complete the token association within the 60-day timeframe results in automatic deletion of the account by NMCI. Subsequently, a new account request will be necessary, and this process will once again take approximately one to five business days for creation.

d. Each echelon V and higher command is required to have a minimum of two TAs. Local TAs are authorized to request tokens from the Local Registration Authority (LRA) once the individual requiring a token has been granted a SIPRNET account. The LRA will generate the token and send the Personal Identification Number (PIN) (which enables token login to workstations) to one of the TAs. Subsequently, a different TA (to avoid accessing both PIN and tokens) will receive and manage the token.

(1) Alternatively, local TAs can request the SIPR Token Certificate Registration Instruction (CRI) from the LRA after the individual obtains their SIPRNET account. The TA will use the provided CRI to create the token and ensure its delivery to the user.

(2) The command's TA will coordinate with the ISSM or ISSO to activate the account through NMCI using an Excel spreadsheet on SIPRNET provided by COMNAVRESFOR LRA. This spreadsheet will include the user's Login ID and Department of Defense (DoD) ID with PCC code.

(3) Following the association of a new account with a token, Navy Reserve Force members must log in every 60 days to prevent account deactivation and every 180 days to prevent account deletion. In case of account locking due to user errors (such as repeated incorrect PIN inputs), members can restore access by contacting NMCI.

(4) If an account becomes disabled due to inactivity, an ISSM or ISSO should reach out to NMCI to restore it. In the event of account deletion, the entire process must be initiated once again. It's important to note that this account deactivation and deletion policy is subject to potential changes.

4. Account and Token Association.

a. The Navy Reserve Force constitutes a geographically dispersed force comprising active-duty personnel, SELRES members, and civilians. This gives rise to complexities for echelon V NRAs when it comes to arranging scheduled interactions with the entire force. Consequently, the process of finalizing NMCI SIPR accounts requires careful planning and synchronization involving supported commands, the Reserve Program Director (RPD), echelon IV Navy Reserve Region Readiness and Mobilization Commands (REDCOMs), as well as echelon V NRAs. Their collective efforts are essential to successfully carry out the aforementioned tasks within the specified time limitations.

b. Upon the issuance of a token, individuals will keep it throughout transitions between different commands and network enclaves. This token will remain in their possession until separation from the service since it does not have an expiration date. However, it will need certification updates every three years. Should a token be returned in undamaged condition, it is eligible for reuse. Not all members receive tokens upon check in due to the minimum clearance prerequisites and the principle of "need to know." In instances where a token was not provided during accession but becomes necessary for a SIPRNET account later on, the responsibility falls upon the supporting NRA or the local COMNAVRESFOR command to provide the token.

c. To facilitate access to SIPR for Navy Reserve members, specific requirements must be conveyed from supported commands through their designated Reserve Program Director (RPD) to echelon V Navy Reserve Activities (NRAs) and the relevant total force member. The responsibility lies with the RPD of the supported command to incorporate these prerequisites into official orders, encompassing scenarios such as active-duty operational support, recalls, Annual Training (AT), or Active Duty for Training (ADT). It is imperative that members fulfill these prerequisites prior to the execution of their orders. For billets involving Inactive Duty for Training (IDT) that need SIPRNET accounts for task execution, the supported command's RPD will outline the SIPRNET stipulations within the job description within My Navy Assignment (MNA) for enlisted billets, or within the supported command comments in Reserve Force Manpower Tools (RFMT) for officer billets. The creation of NMCI SIPRNET accounts and the issuance/distribution of tokens will be overseen by the member's supporting NRA or the local COMNAVRESFOR command, particularly when the member is not situated at their designated unit's present location. NRAs must ensure procedures are in place to locally, or via regional REDCOM, provide SIPR tokens for SELRES personnel who physically drill at the Navy Reserve Centers. Other NRAs can be leveraged to act as cognizant TAs for the purpose of issuing SIPR tokens but must only be leveraged on a case-by-case basis in an emergent situation after consulting with COMNAVRESFOR KMI leadership and the supporting NRA KMI team. NRAs should possess the capacity to establish NMCI SIPRNET accounts and correlate SIPRNET tokens accordingly. In cases where NRAs face challenges in providing on-site NMCI SIPRNET accounts and tokens, including SIPRNET token association, COMNAVRESFOR N6 can provide limited assistance. However, due to the limited availability of tokens, COMNAVRESFOR N6 cannot furnish tokens for the entire Navy Reserve Force. Refer to APPENDIX C "Process for Command TAs To Stand Up or Request SIPR Account/Tokens" for further information/guidance.

5. SAAR-N Forms. Access to any DoD system need the submission of SAAR-N forms. Within the Department of the Navy (DON), these forms are specifically identified as SAAR-N forms (as indicated by OPNAV 5239/14 (09-11)). Thorough completion of

sections 1 to 3 of the SAAR-N forms is mandatory, and these completed forms must be retained in their entirety within the records of the local command. To ensure the integrity and authenticity of the process. See Chapter 3, paragraph 8 for information on management of SAAR-N forms.

6. Defense Enrollment Eligibility Reporting System(DEERS)/RAPIDS (Other Accounts). DEERS or RAPIDS workstations are designated as Programs of Record (POR). They require direct connectivity to the Building Area Network (BAN), Local Area Network (LAN), or Wide Area Network (WAN). The echelon IV, specifically the REDCOM and COMNAVRESFOR N6 staff, holds the responsibility of including contract line-item number (CLIN) X006AR (Program of Record Wall Plug Upgrade or its contract equivalent) in a task order via the NMCI ordering process. Oversight and maintenance of DEERS or RAPIDS terminals fall under the purview of the Defense Manpower Data Center (DMDC). Any concerns related to the system and its associated peripherals should be directed to the DMDC helpdesk at 1 (800) 372-7437. Matters such as the addition or removal of RAPIDS sites, as well as the relocation of RAPIDS machinery and equipment, should be addressed to the Navy Reserve project office via: navyreserveprojectoffice@navy.mil COMNAVRESFORCOM Data Integrity and Reserve Systems (N1C4) Navy RAPIDS sites that operate beyond NAVRESCENs (such as the Transactional Support Center (TSC)) can reach out to the Navy Project Office at (901) 874-4862.

7. Government-Furnished Equipment (GFE) Mobile Phones, and Mobile Cellular Data Device (MCDD)

a. GFE Phones. The issuance of phones will adhere to the guidelines outlined in the Continental United States Wireless Communication Support Services Policy dated 30 July 2019. This policy document is available on the COMNAVRESFOR (N63) CTR page located on Navy Reserve Homeport under the section dedicated to Wireless Documents.

b. Mobile Cellular Data Device (MCDD). MCDD requests require justification and endorsement by the appropriate Chief Staff Officer. Issuance of MCDDs is exclusively managed by COMNAVRESFOR N6 and cannot be funded through local Operating Target (OPTAR) budgets. Send requests to: navresformobiledevices@us.navy.mil

c. COMNAVRESFOR N6 holds the authority for all echelon IV and V commands to approve the utilization of the MCDDs in conjunction with NMCI laptops. Issuance of MCDDs is exclusively managed by COMNAVRESFOR N6 and cannot be funded through local OPTAR budgets.

8. Nautilus Virtual Desktop (NVD). Nautilus is a Navy Flank Speed service, which uses Microsoft Nautilus Virtual Desktop (NVD) technology. This service is tailored for individuals lacking continuous access to NMCI, not possessing Government Furnished Equipment (GFE), or those who opt to utilize their personal Bring Your Own Device (BYOD). Reserve members are empowered to work remotely from any location they choose through the NVD platform. Personnel will access the provided request form through the link below using your Flank Speed account and complete the form. It's important to note that the initial setup process for NVD does require one-time access to either an NMCI computer or GFE. Upon approval of your request, volunteers will receive a welcome/onboarding email from the NVD Team: https://forms.osi.apps.mil/r/jJjKgQY6th. If you need to reset your password, please follow the steps below:

a. From a personal laptop: Click on the first link to start the 15-minute timer, then click on the second link to reset your password in GFUD. Once you reset your password, wait about an hour and try logging in. If you are still having issues, repeat the process one more time.

(1) Non-DoDIN Step 1: Start the 15-minute Timer (sharepoint-mil.us)

(2) Non-DoDIN Step 3: Set Your SSPR Password (sharepoint-mil.us)

b. From an NMCI machine (or GFE): Click on the link below to visit the GFUD website and "Set your Password" from there. https://portal.apps.deas.mil/

9. Message Traffic. All commands will maintain their own Plain Language Address and the ability to transmit and receive message traffic (C2OIX) on both NIPRNET and SIPRNET.

10. COMNAVRESFOR Customer Support Center (CSC).

a. The CSC provides support for all headquarter (HQ) IT requirements and computer management to include but not limited to: HQ on-site assistance, Navy Message Traffic (COMNAVRESFOR, COMNAVRESFORCOM, Commander, Naval Air Force Reserve), teleconference/VTC/conference scheduling and support, and Force wide support (as required that cannot be resolved at the command/REDCOM level).

b. The CSC does not provide support for non-NRH hosted applications.

c. The CSC maintains a SharePoint Knowledge Management page which supports standard operating procedures for common troubleshooting, IT support requests, HQ conference room requests, teleconference requests and application development support. The CSC Knowledge Management page is located at:
https://private.navyreserve.navy.mil/sites/helpdesk/Pages/Customer%20Support%20Center.aspx

d. Provides monthly SharePoint training available to all Reserve Forces to enhance NRA/Unit SharePoint management and standardization. Registration is located at:
https://private.navyreserve.navy.mil/coi/SPTC/Pages/default.aspx.

11. Very Important Person/Distinguished Visitor/Flag Officer IT Support.

a. In the event a Navy Reserve Flag Officer is in residence and requires assistance with NMCI related computers, the NMCI VIP Service is available at 1 (877) 274-8783.

b. The COMNAVRESFOR DCTRs will procure, deploy, and provide equipment and customer service, to include follow-up on NMCI trouble tickets, to all flag officers attached to or working with any COMNAVRESFOR command, as required.

c. COMNAVRESFOR Flag VIP Program is ultimately managed by COMNAVRESFOR N6. Tasking and fielding of requests are handled by the designated proxy/proxies for each VIP which is set by the Authorized Proxy Management Tool in HP Service Manager.

d. Only the COMNAVRESFOR N6 has permissions to set the proxy or proxies for each individual Flag VIP. Request for changes/updates to respective proxy list should be requested via the NRH ticket portal.

CHAPTER 2

FACILITIES AND BUDGETARY GUIDELINES

1. NIPRNET Computers. All commands attached to COMNAVRESFOR will adhere to the following updated baseline ordering model to meet NIPRNET computing and connectivity requirements. Direct all requests for explanation of this guidance to the COMNAVRESFOR NMCI Information Technology (IT) Operations Manager (N63).

a. Budget Guidelines. COMNAVRESFOR N6 manages the claimant wide NMCI budget. Commands may make changes to their NMCI task order, but additions will be authorized by COMNAVRESFOR (N63) to ensure the change remains within the authorized budget. All conditions of this instruction are dependent on the availability of funding.

b. Ordering Guidelines. The ordering guidelines are a framework for assisting the REDCOMs in calculating the suggested computer allowance for each type of command in their area of responsibility. For the purpose of this subsection, Navy civilians and permanent contractors are considered TAR. These guidelines will be re-examined when new contracts are put in place.

(1) Echelon 2 through 5:

(a) One (1) NMCI seat for each TAR member.

(b) One (1) NMCI training seat for 12 SELRES as fiscal resources permit.

(2) Commander, Naval Air Force Reserve Command Aviation Supply Departments (ASD)/Fleet Readiness Commands (FRC):

(a) One (1) NMCI seat for each TAR officer.

(b) Two (2) NMCI seats for every three (3) TAR enlisted.

(c) One (1) NMCI training seat for 12 SELRES as fiscal resources permit.

(3) Navy Reserve Echelon 6 Commissioned Units:

(a) One (1) NMCI seat for the unit (CO).

(b) One (1) NMCI administrative seat. This seat can be either a portable or fixed seat.

(c) Additional seats can be requested via the Echelon 3 through 5 chains of command to support unit-specific requirements and/or mobilization readiness.

2. SIPRNET Computers. A minimum of one SIPRNET seat is required for each echelon IV and V command. This requires a secure enclave. If the command does not have a secure enclave, they must have a Memorandum of Agreement (MOA) with a nearby facility that will provide SIPRNET access. For more information pertaining to secure enclave requirements see Chapter 2 Space Certification and Chapter 3 KMI.

3. Desktop Phones. Ordering and repair processes and general responsibility for normal desktop phones reside with the host service e.g., U.S. Air Force Reserve, Commander Navy Installations Command (CNIC) or Base Communications Office (BCO). When services are transferred to the Enterprise Infrastructure Solutions contract, general responsibility will reside with COMNAVRESFOR.

4. VOIP Phones. For sites with Echelon II/III approval Voice Over IP systems are being installed to replace legacy phone service. Sites that are hosted by a DoD installation will need to verify the hosting source for VOIP services, as some tenants may receive service as part of a lease agreement. For those sites hosted by COMNAVRESFOR, please use the resources located on the FlankSpeed SharePoint Online site for troubleshooting, system operations, etc.

Site Link: Click Here

5. Printing Services. Per reference (a), COMNAVRESFOR is limiting the procurement of all networked and stand-alone DON pre-Next Generation Enterprise Network (NGEN) contract- procured Single-Function Devices (SFDs) copiers, printers, fax machines, scanners, Multi- Function Devices (MFDs), and related consumables and support services. This policy applies to all Echelons of COMNAVRESFOR. COMNAVRESFOR N6 has determined, and the DON Chief Information Officer (CIO) has established the Defense Logistics Agency (DLA) as the single manager for printing and high-speed/high-volume duplicating, and the preferred provider of document conversion and automation services. Per reference (n), the Deputy Department of the Navy Chief Information Officer-Navy (DDCIO-N) has directed all echelon II commands to use DLA Services in alignment with DON CIO policy, as noted above. The overall objective is to achieve cost savings associated to consumables and maintenance at reduced cost. MFD implementation plan is as follows:

a. New requirements for office printing, scanning and photocopying of unclassified documents will be met by purchasing a MFD. Detailed written guidance to assist with the leasing process associated with MFDs can be found on the COMNAVRESFORCOM Operations/NGEN (N63) CTR page on Navy Reserve Homeport.

b. New requirements for office printing, scanning, photocopying and faxing of classified documents will **NOT** typically be met by use of MFDs.

c. Existing SFDs will continue to operate until service life is met or a determination is made by the local command that the cost of supplies and maintenance would be greater than ordering a DLA MFD replacement.

d. SFDs that fail will be replaced by a DLA MFD as long as the procurement is within the bounds of the DLA assessment of the local command.

e. Should the DLA be unable to support a SFD request, consideration for purchase of a SFD will have a DLA written waiver of approval to procure the device from another vendor. An Information Technology Procurement Request (ITPR) is required for the purchase of the new

f. SFD and COMNAVRESFOR will meet the requirements as set forth by the Chief of Naval Operations (CNO) as well as that which is required by the ITPR process. The SFD purchased, via a DLA printer waiver, will also be listed on the NMCI Certified Device List. The waiver will be attached to the ITPR and cannot be a network device. Reference (x) provides further detail.

g. SFDs in the same office work area as a DLA MFD will be removed from service to the maximum extent practical to conserve resources. The MFD takes precedence over the SFD.

h. SFD copiers are on a separate DLA lease contract and can be operated until the cost/benefit of paying the DLA penalty fee for breaking the lease is more cost beneficial than having a MFD and a SFD copier on two separate contracts simultaneously. The MFD takes precedence over the SFD.

i. Unclassified MFD in SIPR spaces. MFDs are authorized for SIPR processing only with prior N63/N64 approval. Requests for SIPR MFDs must include a justification routed through the chain of command detailing why a SFD will not suffice and a mitigation plan to prevent a classified spillage from occurring."

6. Open Secret Storage (OSS) Certification.

a. There are two different types of secure spaces that require certification in order to store or use Communications Security (COMSEC) material within the Navy Reserve. Fixed COMSEC facilities and OSS. The fixed COMSEC facilities require certification/re-certification through the Naval Communications Security Material System (NCMS) process using the Immediate Superior in Command (ISIC) inspector as the certifying official. Facilities must meet the requirements outlined in CMS-1 (series) instructions for storage and processing of COMSEC material. OSS spaces are certified/re-certified by the CO or security manager and must meet the requirements outlined in CMS-1 (series) and reference (v) instructions. These types of spaces do not process or generate COMSEC material and should be treated and certified as such. COMNAVRESFORCOM NRAs with secure spaces will certify them as OSS spaces. With both types of spaces, the Secure Room (SR) checklist must be filled out by the local command hosting the facility and sent to COMNAVRESFORCOM N6 KMI team. This checklist will be held in the command's folder and utilized to generate the process of certification of the space to hold/process COMSEC material.

b. Once both types of spaces meet all requirements for certification, a designation letter will be generated either by the ISIC inspector in the case of fixed COMSEC facilities, or by the CO/security manager at the local command for OSS. This letter will be held (along with the SR checklist) both at the command in the secure space and by the COMNAVRESFORCOM N6 KMI Team. Until all conditions have been met the local command cannot maintain COMSEC material.

c. The OSS certification program is a physical security program of which is owned and managed by the Regional Security Managers and the Force Security Manager.

d. For additional details, contact your Regional Security Manager.

7. Military Construction (MILCON) and Facility Restoration.

a. MILCON. When a new Reserve Facility is approved through MILCON appropriations, it is the REDCOM's responsibility to ensure that IT requirements are considered. Specific requirements should be vetted during the planning phase to ensure the new construction will adequately meet the needs of the Reserve Facility. ECH 3-4 will track the progress of the new facility and order a site survey at the anticipated 80 percent completion date. Post site survey, the ECH 3/4 will submit a CLIN600 and keep COMNAVRESFORCOM (N63) apprised of any changes or delays.

b. NAVRESCEN Rehabilitation. When a Reserve facility is approved through MILCON appropriations for rehabilitation, it is the REDCOM's responsibility to ensure that IT requirements are considered. Specific requirements should be vetted during the planning phase to ensure the new construction will adequately meet the needs of the Reserve Facility. The REDCOM will track the progress of the new facility and order a site survey at the anticipated 80 percent completion date. Post site survey, the REDCOM will submit a CLIN600. REDCOMs will keep COMNAVRESFORCOM (N63) apprised of any changes or delays.

CHAPTER 3

MANAGEMENT RESPONSIBILITIES

1. Introduction. COMNAVRESFOR N6 functions as the echelon II and echelon III IT department for COMNAVRESFOR. COMNAVRESFOR N6 is responsible for the Force IT operations and Force IT budget execution. Reserve ECH 3-4 commands will be responsible for the administration of every COMNAVRESFOR command within their geographic region for all matters concerning Navy Reserve IT and related services, including NMCI. Exceptions are Office of the Chief of Navy Reserve Staff Detachment, Commander, Naval Information Force Reserve, Navy Air Facility Washington, Navy Air Logistics Office, and Navy Reserve Professional Development Center will be responsible for managing NMCI in their cognizant areas within COMNAVRESFOR.

2. System Change Requests.

a. IT change requests may be submitted to COMNAVRESFOR N6 via the procedures defined in the COMNAVRESFOR N6 configuration management plan located on the Navy Reserve Homeport N6 page at the following location: https://private.navyreserve.navy.mil/COMNAVRESFORCOM/N-Codes/N6 under the N6 IT policies tab. IT change requests will fall into one of two categories; enhancements to current capabilities or new requirements. Enhancements will encompass proposed upgrades to the COMNAVRESFOR IT enterprise including processes, hardware, software, and documentation. New requirements include requests for digital capabilities and solutions, features, functionality, documentation, hardware, or software that are not currently in the COMNAVRESFORCOM IT enterprise.

b. The COMNAVRESFOR N6 IT Configuration Control Board (CCB) is the official mechanism for controlling changes to the configuration baseline of the COMNAVRESFORCOM IT enterprise, and it is the governing body chartered to ascertain all impacts of proposed changes. The CCB provides necessary prioritizations for all significant IT change requests as well as executive oversight for change management. The CCB also ensures that changes are made in a controlled manner and are documented in the operational architecture. All COMNAVRESFOR commands and activities will utilize the COMNAVRESFOR N6 IT CCB as the authoritative source for COMNAVRESFOR IT enterprise configuration changes. The CCB will be tasked to review, approve, and prioritize incoming IT change requests. The COMNAVRESFOR N6 configuration manager will determine which requests are routed to the CCB via the local CCB. Meetings will include the request originator and COMNAVRESFOR stakeholders as needed to ensure that the interests of their respective organization(s) are represented. The COMNAVRESFOR N6 IT CCB is established to serve the following purposes:

(1) Represent the interests of all groups who may be affected by changes to the baselines.

(2) Authorize the creation of products from the baseline library of the COMNAVRESFOR IT enterprise.

(3) Evaluate and approve or disapprove proposed changes to controlled configuration items.

(4) Prioritize approved changes.

3. IT Inventory. Inventory of NMCI NIPRNET/SIPRNET computers, such as NMCI desktop computers and laptops, and other IT computers, such as MFDs, MCDDs, GFE cell phones, and smart phones, and software licenses will be required of Reserve ECH 3-4 commands in conjunction with their subordinate commands on an annual basis at each change of command or as scheduled by COMNAVRESFOR. Corrections to errors will be made in the NET as the sole authority on that data. Reserve ECH 3-4 personnel completing IT inventories and working with NET are to complete NET training via the CTR training page on the NMCI Homeport.

4. Non-NMCI IT Procurement Requests. All non-NMCI IT purchases, regardless of cost, are required to be submitted and an approved ITPR via the Navy Information Technology Approval System (NAV-ITAS), see reference (w) for further details. Find additional NAVITAS documentation and guidance located at: https://private.navyreserve.navy.mil/COMNAVRESFORCOM/N-Codes/N6/COMNAVRESFORCOM_N63_CTR/Pages/default.aspx

5. NMCI Services Request (CLIN600)/Requirement to Award Process Tool (RAPT) Infrastructure.

a. RAPT is a Contracts application which documents the requirement approval and Procurement Contracting Office (PCO) acquisition process and serves as the NMCI electronic contract file. Typically, CLIN CLIN600's are used to make changes to the NMCI infrastructure. This can be as simple as adding a new blade to an existing switch to a more complex project such as establishment and wiring a new building. CLIN600's can also be used to install new wall drops in conjunction with a switch installation for easier project management.

b. Contact your CTR for assistance in creating a CLIN600 RAPT Request. The purpose of the RAPT Request is to automate the approval and negotiation processes for unpriced requests and general contracting actions. The tool is created around basic workflow functionality where CTRs create requests by completing questionnaires that are then routed through an approval process. The RAPT process consists of requirements generation, claimant approval, technical evaluation, price analysis, contract negotiation, and award. The tool provides a repository of approved, rejected requests, and corresponding document repository as a record. CLINs (or contract equivalent) are created as a result of an awarded request and are written to NET, where they are enabled for ordering.

c. The CLIN600 process is started by procuring a survey and a travel CLIN (or contract equivalent (if required) and submitting the CLIN600 (or contract equivalent) survey form which will result in a working rate card (WRC). The command will open a CLIN600 RAPT (or contract equivalent) request upon receipt of the WRC. Submission of the RAPT request will result in award of orderable CLINs (or contract equivalent) for the project. The command must order the CLINs (or contract equivalent) for the vendor to start the work.

6. Account Management, ISSM/ISSO Responsibilities, LRA, and TA.

a. ISSM (ECH 2/ECH 3) responsibilities.

(1) Ensure that all cybersecurity components have completed the appropriate evaluation and configuration processes prior to incorporation into or connection to an Information System (IS) or Platform Information Technology (PIT) system.

(2) Be trained, qualified, and appointed in writing by the commanders of DON organizations.

(3) Develop and maintain an organizational or system-level cybersecurity program that includes cybersecurity architecture, requirements, objectives, policies, cybersecurity personnel, cybersecurity processes, and procedures.

(4) Maintain a repository for all organizational or system-level cybersecurity-related documentation.

(5) Ensure that ISSOs are appointed in writing and provide oversight to ensure that they are following established cybersecurity policies and procedures.

(6) Monitor compliance with cybersecurity policy and review the results of such monitoring.

(7) Ensure that cybersecurity inspections, tests, reviews are scheduled, synchronized, and coordinated with affected parties and organizations.

(8) Ensure implementation of security measures, procedures, including reporting incidents to the commander, command security manager, appropriate reporting chains, and coordinating system-level responses to unauthorized disclosures per applicable DoD instructions, directives, and notices.

(9) Periodically assesses the quality of security controls implementation against performance indicators, such as security incidents, feedback from external inspection agencies (e.g., Office of Inspector General (OIG) DoD, Government Accountability Office (GAO)), exercises and operational evaluations, including director, Operational Test and Evaluation (OT&E), IA, assessments.

b. ISSO (Echelon 4-5) responsibilities:

(1) ISSO serves as the principal advisor to the ISSM on all matters, technical, and otherwise, involving the security of an information system. The ISSO typically has the detailed knowledge and expertise required to manage the security aspects of the information system and, in many cases, is assigned responsibility for the day-to-day security operations of the system.

(2) This responsibility may also include, but is not limited to, physical security, personnel security, incident handling, and security awareness and training. The ISSO may be called upon to assist in the development of the system security policy and to ensure compliance with the policy on a routine basis.

c. Local Registration Authority (LRA) responsibilities.

(1) The LRA's primary responsibility is to properly register users in the PKI system, so users can obtain PKI certificates. This involves verifying a user's identity and entering the user's information in a special LRA application on the LRA's workstation. LRAs do not need to directly manage or keep track of user keys and certificates however, there are occasions when a user's certificate must be revoked, and/or a new certificate for the user is required. The LRA provides support in these circumstances.

(2) Informing users of their responsibilities (DD-Form 2842 (08-09)).

(3) Assisting users with the management of keys and certificates.

(4) Managing a central workstation for registration (if the site requires one).

(5) If a REDCOM does not currently provide LRA services, REDCOMs then should contact NCMS LRA (NCMS_SDAS_PKI@us.navy.mil or NCMS_NRFK_PKI_AUDITORS@NAVY.MIL) requesting information to stand up an LRA program. REDCOMs should provide LRA services for NMCI SIPR access for all echelon V NRCs and NRAs.

d. TA responsibilities.

(1) REDCOMs or NRCs who do not have a TA program will submit a request with COMNAVRESFOR LRA to establish a TA program. This program will provide immediate assistance to Reserve members who require SIPR Account and SIPR Token creations/activations/re-enablements.

(2) A TA is an individual who supports an LRA by performing the face-to-face user authentication and handing out the Certificate Registration Instruction (CRI) forms for the LRA. The TA concept allows easier registration of users at remote locations, where it may be impractical for the user to come in person to an LRA or vice versa.

(3) Validation that the subscriber is eligible to be registered (U.S. Military, DoD civilian, contractor, or others using government furnished equipment and working in government spaces).

(4) Gathering and forwarding subscriber registration information to the LRA.

(5) Delivering certificate CRI and initialized tokens or keyed tokens and/or activation data to subscribers.

(6) Verifying the identity of each subscriber as specified in Section 3.2.3 of the DoD Registration Practice Statement (RPS).

(7) Assist subscribers in the downloading and installation of their certificates.

(8) Reporting to the LRA if a subscriber suspects a compromise or loss of a private key.

(9) Note: See APPENDIX C for additional information pertaining to the Trusted Agent program.

7. SAAR-N forms. SAAR-N forms are a prerequisite for access to any DON system. SAAR-N forms Parts I-III are required to be completed in full and kept on file by the local command. Digital signatures will be used to provide non-repudiation. A favorable Tier 3 (minimum level) is required for unclassified network access due to access to privacy act/PII or propriety information residing on networks. For military/government employee members, in most cases network access may be granted if their investigation has expired but should contact their security office for reinvestigation submission. For military, government employees, and contractors, in instances where no investigation was ever started, an investigation will be initiated and completed for review and temporary eligibility issuance before permitting unclassified network access to personnel. If personnel have a denied or revoked eligibility status, their NMCI account will be disabled until the status is satisfactorily resolved through the mitigation, appeal or reconsideration request process. SAAR-N Part IV will be completed as required. Commands will retain electronic SAAR-N forms for one year after user account is terminated or when no longer needed for investigative or security purposes, whichever is later.

8. Key Management Infrastructure (KMI). KMI formerly Electronic Key Management System (EKMS) is designed to provide COMSEC. Examples include Tactical Local Area Network Encryption (TACLANE), Secure Telephone Equipment (STE), and more.

a. SIPRNET capability is for secure internal communications only for both the RC and AC. COMNAVRESFOR is not funded for additional SIPR seats to support gaining commands. However, if an NRC wants to add SIPR seats, it may do so provided it can obtain one or more of the following:

(1) COMNAVRESFOR N6 authorization.

(2) Has sufficient space in its secure enclave for additional drops and seats.

(3) Has sufficient space available on the switch.

(4) If in support of a gaining command, obtain funding from the gaining command.

b. COMNAVRESFOR commands will maintain SIPRNET capability. All sites require 24/7 access to SIPRNET. If a command does not have on-site access, then steps will be taken to meet SIPR requirements. If a command is unable to meet these requirements but can procure access via another acceptable DoD facility within a 50-mile radius, requirements can be satisfied with a Memorandum of Agreement (MOA). The MOA shall be reviewed, approved, and signed by the requesting Commanding Officer (CO) and the local commands CO. This MOA is required to be updated upon a change of command for either command. After the MOA is approved and signed, the respective Reserve ECH 3-4 will file a copy for reference.

c. Reserve ECH 3-4 commands and NRC COs have the authority to request for COMNAVRESFORCOM KMI program disestablishment by submitting a written request to COMNAVRESFORCOM N64 Staff Communications Material System Responsibility Officer (SCMSRO). Justification and understanding of accepting potential risks must be provided.

(1) If approved (OCNR), the command shall have an MOA in place with a local command to ensure 100% SIPR accessibility in support of the warfighting mission for the Reserve FORCE.

d. COMNAVRESFORCOM is the KMI parent account (for all subordinate commands who currently possess COMNAVRESFORCOM KMI COMSEC equipment). These commands are referred to as Local Elements (LE). If a command possesses COMSEC material provided by COMNAVRESFORCOM KMI (TACLANEs, STEs, etc.) a Memorandum of Understanding (MOU) is required. Digital signature or black ink are authorized. The LE CO and COMNAVRESFORCOM SCMSRO are the only members who are authorized to sign the MOU. The LE Custodians of each command are required to review the MOU with the intent of understanding all requirements and expectations. The CO has ultimate responsibility for managing and overall conduct of the KMI LE account.

(1) The MOU is a formal agreement between the LE CO and COMNAVRESFORCOM SCMSRO outlining required COMSEC duties and responsibilites

(2) All Reserve ECH 3-4 commands and NRCs shall have a minimum two LE custodians, E-5 and above or E-4 and below with a waiver, (the CO is not authorized to act as a LE custodian). These members will administer the equipment and material. They will be formally qualified upon completing the following requirements IAW CMS-A AMD-1; KMI 301 PQS training and exam (minimum passing score is 80%), SD-572, Annex-J, Designation Letter, and E-4 and below waiver (if applicable).

(3) COMNAVRESFORCOM KMI provides KMI 301 PQS training twice per month and is advertised on the COMNAVRESFORCOM KMI SharePoint homepage. Requesting attendance via COMNAVRESFORCOM KMI's SharePoint page is the only authorized method.

(4) Change of command responsibilities. A 30-day notice shall be provided to the COMNAVRESFORCOM KMI team to ensure an inventory (SF-153) is completed during the official Change of Command (CoC) turnover process. The following documents are required to be updated/completed within 30 days of the CoC: MOU, Designation Letters, Access List, the CO's SD-572, Annex J and LE Questionnaire.

(5) Semi-Annual Inventory. SF-153s are only generated by the COMNAVRESFORCOM KMI Team. Commands outside of COMNAVRESFORCOM KMI are not authorized to generate an SF-153. All LEs shall conduct inventories on the provided SF-153 for their accountable material to COMNAVRESFORCOM KMI team every January and July or when otherwise directed. A Non-Reportable PDS will be issued for those commands who failed to complete and upload the SF-153 by the deadline COMNAVRESFORCOM KMI determines.

(6) Semi-Annual Self-Assessments. LEs shall conduct a self-assessment every January and July or when directed. All questions (A, I, P) of the CMS-3A AMD-1 Annex B must be answered. Questions that are N/A are required to be answered accurately. Annex B encompasses sections (1-3) and subsequent tabs of each section. A Non-Reportable PDS will be issued for those commands who failed to complete and upload the entire Annex B with authorized signatures by the deadline COMNAVRESFORCOM KMI determines.

(7) Annual Rekey. All LEs are required to turn in TACLANEs each year to the COMNAVRESFORCOM KMI team for rekey. STEs shall be rekeyed at the local command unless otherwise directed by COMNAVRESFORCOM SCMSRO or the KMI team. This must be completed each year by the end of April. COMNAVRESFORCOM KMI will provide guidance annually for the rekey evolution.

(a) TACLANE requirements. Not adhering to the above statement (Annual Rekey), a Command can incur a COMSEC Incident if the Command fails to remove the TACLANE from the server prior to the last day of the assigned month and lets TACLANEs operate on expired crypto.

(b) STE Phone and KSV-21 requirements. Not adhering to the above statement (Annual Rekey), a Command can incur a COMSEC Incident if the Command tries to conduct secured phone calls after the deadline without conducting rekey properly.

(8) Additional KMI requirements.

(a) Les are required to provide monthly connectivity updates via SIPR e-mails and STE calls (secure).

(b) Participate in monthly training held by COMNAVRESFORCOM KMI as well as additional training/general meetings your respective ECH 3-4 N6s require.

(c) Conduct Quarterly Spot Checks IAW CMS-3A AMD-1 Annex B. All questions (A, I, P) of the CMS-3A AMD-1 Annex B shall be answered. Questions that are N/A are required to be answered accurately. All tabs of each Section are required to be fully completed and uploaded onto COMNAVRESFORCOM KMI's SharePoint page by the deadline to ensure full compliance. A Non-Reportable PDS will be issued for those commands who failed to complete and upload the correct Spot Check with authorized signatures by the deadline COMNAVRESFORCOM KMI determines.

(d) Other set requirements delineated in each MOU, CMS-1 (Series) literature, and COMNAVRESFORCOM KMI team guidance.

9. Collaboration Tool: NRH SharePoint Portal.

a. Landing Page. Considered to be the first viewable page for each command. Each section of the landing page will adhere to the COMNAVRESFOR approved layout. This page will contain:

(1) Command name.

(2) Mission statement.

(3) Easy tab section 1.

(4) Leadership section with photos and biography links.

(5) Plan of the month.

(6) Drill schedule.

(7) Staff directory.

(8) Command profile (address, hours of operation, contact phone numbers, command logo).

(9) Easy tab section 2.

(10) Announcements.

(11) Command calendar.

(12) Hyperlinks to site owner to a valid and official Navy e-mail address.

(13) Command Interactive Customer Evaluation link (ICE) must be hyperlinked to a valid ICE comment card.

(14) COMNAVRESFOR maintained required awareness logos (i.e., Sexual Assault Prevention and Response, Anti-Terrorism and Force Protection, Suicide Prevention).

(15) SAPR POC: must contain information for three points of contact. Local contact information from the command must be used unless unavailable. Regional contact information may be used if local representatives are not present

(16) Additional site pages are authorized as required by each command

b. New Site Requests. Creation of sub sites for lower echelon commands requires the completion and submission of a site request form. Site requests must be sent to the respective ECH 3-4 command for approval and forwarded to the COMNAVRESFOR helpdesk via the CSC ticketing system. Sites created by personnel other than COMNAVRESFOR N6 personnel are not authorized and may be subject to deletion. The site request from can be located here: https://private.navyreserve.navy.mil/COMNAVRESFORCOM/N-Codes/N6/sharedservices/Pages/NRH-Standardization.aspx

c. Standardization. Reserve ECH 3-4 commands will monitor and validate site standardization for lower echelon commands. All sites and sub sites standardization will be tracked via the NRH standardization tracker located at the following web address: https://private.navyreserve.navy.mil/COMNAVRESFORCOM/N-Codes/N6/sharedservices/Pages/NRH-Standardization.aspx

d. Standardization Review. COMNAVRESFOR N6 SharePoint administrators will conduct monthly standardization and compliance audits accounting for 10 percent of site collections on NRH. Failure to correct discrepancies may result in site deletion or suspension.

e. Site troubleshooting. Troubleshooting SharePoint related items should be handled at the lowest echelon level as required using the IT chain of command.

f. Site permission management. To verify each person is assigned appropriate privileges/permissions, each command will validate its subordinate command's assignments to site owner roles. Example: REDCOMs will validate NAVRESCENs; NAVRESCENs will validate Reserve Units. The permission level "full control" will be limited to COMNAVRESFORCOM N6 personnel.

(1) Community of Interest site permissions (full control) will be approved and maintained by submitting a ticket to COMNAVRESFOR's helpdesk. Submitted tickets will include parent site URL, for which permissions are being requested.

(2) Other permissions will be maintained by local SharePoint site owners but maybe validated at any time by reserve ECH 3-4 commands or COMNAVRESFORCOM N6 personnel.

g. SharePoint training. Review of SharePoint training presentations are required by all personnel prior to receiving permissions to author, manage, or contribute site information.

(1) SharePoint site owners are required to review SharePoint training levels 100, successfully

(2) pass a SharePoint standardization test or attend the COMNAVRESFORCOM N6 SharePoint two-day course prior to receiving "Full/Site Owner" permissions. Training presentations and training schedule are located on the N6 SharePoint page at https://private.navyreserve.navy.mil/coi/SPTC/Pages/default.aspx

(3) Personnel requesting "Content" permissions are required to review SharePoint training level 100 prior to receiving full or contribute permissions. The COMNAVRESFOR training schedule and additional SharePoint training monthly for standardization testing and training. The training schedule can be found at https://private.navyreserve.navy.mil/coi/SPTC/Pages/default.aspx

h. User profile synchronization. All military, government civilian, or contractor personnel requiring access to SharePoint will have a (.mil) or (.gov) e-mail address associated to his or her profile.

(1) SharePoint user profiles (display name, phone number, e-mail address) will automatically update via the user profile synchronization for users who maintain a NMCI e-mail account.

(2) Non-NMCI users will be required to contact COMNAVRESFOR's SharePoint helpdesk for manual updates to their SharePoint User Profile (display name, phone number, e- mail address).

i. Linking ".COM" Websites. Linking of ".COM" websites or links will be allowed on SharePoint pages only if they have a mission need and those sites have been screened/reviewed for associated risks by COMNAVRESFOR (N64).

(1) Posting of official Navy documents or information to non-Federal Risk and Authorization Management Program (FEDRAMP) rated Cloud services or Cloud services that do not meet minimum Cloud security requirements as stated in reference DON CIO Memo. Acquisition and use of commercial cloud computing services, such as Google Drive, Dropbox or Box is prohibited. Documents approved for "official public release" by the Force PAO or PAO representative are exempt.

10. Navy Reserve Force Wi-Fi (NRW) Usage Procedures and User Responsibilities.

a. These procedures will include, but are not limited to, mandatory wireless device set-up requirements for maximum cybersecurity, security, and overall user responsibilities. Only those wireless devices meeting the standards specified in this instruction are approved for connectivity to NRW. The procedures and policy items contained within this document meet the requirements of reference (k).

b. These procedures and user responsibilities apply to all COMNAVRESFOR military, civilian and contract personnel assigned to locations with NRW services installed, system maintainers and managers, all users, and all wireless infrastructure devices connecting to the Wi-Fi network. User access to NRW resources is a privilege. Responsible system management is required to maintain confidentiality, integrity and availability of information computers.

c. Responsibilities.

(1) NRW Program Manager will:

(a) Provide NRW program management and overall risk management.

(b) Coordinate with COMNAVRESFOR ISSM to adjudicate cybersecurity violations related to NRW usage and make recommendations for all cases.

(2) Reserve ECH 3-4 commands will:

(a) Report all cybersecurity violations to COMNAVRESFORCOM ISSM and assist in all administrative matters pertaining to NRW.

(b) Conduct periodic inspections to ensure adherence. Inspections will include, but are not limited to user registration process, physical security of NRW equipment, user conduct in NRW spaces, and signal footprint to ensure broadcast does not bleed into classified spaces.

(c) Maintain situation awareness regarding NRW use at subordinate commands.

(d) Make recommendations to COMNAVRESFORCOM to install new NRW networks at COMNAVRESFOR sites with a high demand signal for network usage or to add Wireless Access Points (WAP) to current site configurations.

(3) NAVRESCEN COs/officers-in-charge (OIC) will:

(a) Implement and ensure adherence to this policy. CO or OIC's direct involvement is required to ensure that security and cybersecurity is maintained.

(b) Enforce strict compliance with NRW usage policy and ensure access is denied to users who violate policy.

(c) Verify physical security of NRW system router in a secure, locked space. Do not permit tampering with system configuration or settings.

(d) Make recommendations to echelon 4 to install NRW at COMNAVRESFOR sites with a high demand signal for network usage or to add WAP to current site configurations.

(4) NAVRESCEN or COMNAVRESFORCOM site ISSM or ISSO will:

(a) Act as designated administrator of the NRW network and take responsibility for implementation of procedures for validating users and wireless devices.

(b) Verify all wireless devices and users are compliant with the requirements delineated in Appendix B of this instruction.

(c) Report any user or device found to be in violation of this instruction or cybersecurity procedures and block the respective device from accessing NRW.

(d) Conduct random walk-through inspections in wireless internet capable spaces to verify proper use.

(e) Ensure physical integrity of the router and its installed peripheral equipment. The router will remain in a locked and secure space. Settings will not be modified without explicit permission from the NRW Program Manager.

(5) NRW users will:

(a) Follow the procedures and policy set forth in this instruction.

(b) Ensure personal computing devices have requisite hardware installed, including a wireless adapter and CAC reader.

(c) Use NRW to connect to .mil, .gov, .edu domains and other authorized internet sites, as set forth in the DON IT Acceptable Use Policy. NRW is only to be utilized for accessing public-facing websites and DoD public-facing CAC-enabled websites.

(d) Ensure no sensitive information, including documents containing PII or Controlled Unclassified Information (CUI), are stored on personal computing devices, including personal hard drives, computer memory, and temporary files.

(6) Troubleshooting Personal Devices. The NAVRESCEN CO, site OIC, or local ISSM/ISSO or CSWF personnel are prohibited from troubleshooting personal computing devices. The vast number of operating systems and hardware configurations loaded on personal computers make this function beyond the scope of CSWF personnel.

(a) Troubleshooting systems is a personal responsibility.

(b) Users bear all risk associated with the use of NRW network. The government is not liable for any damage or loss incurred as a result of network use.

(7) Enforcement. A user found to have violated this policy will have their NRW privileges revoked and may be subject to disciplinary action. Users may be reinstated at the direction of the COMNAVRESFOR ISSM. The level of reinstating authority depends on the nature and scope of the violation. Example violations warranting access denial include:

(a) Improper use of NRW, as defined in the user agreement.

(b) Visiting sites that would bring discredit to Naval Service (e.g., gambling, pornography).

(c) User does not have a current NMCI account.

(d) User is deficient in annual cybersecurity, PII, or OPSEC training.

(e) Other reasons as determined by NRC commander, Reserve ECH 3-4 command ISSM, or COMNAVRESFOR ISSM.

11. Cyber Security Workforce (CSWF).

a. Per DON and DoD requirements, commands must establish and manage a Cyber Security Workforce (CSWF) program to staff, train, and sustain a professional IT workforce with a common understanding of Cyber Security (CS) concepts and principles, and the skills needed to effectively prevent and respond to attacks against government information systems and networks.

b. The cyber-IT/CSWF will be composed of those individuals who perform cybersecurity functions. This includes personnel who secure, defend and preserve data, networks, net-centric capabilities, and other designated systems by ensuring appropriate security controls and measures are in place, and taking internal defense actions. This includes access to system controls, monitoring, administration and integration of cybersecurity into all aspects of engineering and acquisition of cyberspace capabilities. It also includes personnel who design, build, configure, operate and maintain IT, networks and capabilities. This includes actions to prioritize portfolio investments, architect, and engineer, acquire, implement, evaluate, and dispose of IT and services. In addition, it includes information resources management, management, storage, transmission, and display of data and information.

c. Commands will assign at least one cyber-IT/CSWF-PM (appointed by CO) to track and manage their local CSWF program. Military and civilian personnel filling cyber-IT/CSWF positions will obtain the appropriate DON-approved baseline job qualification standards within 6 months of assignment. The CO will ensure that military and civilian personnel are appropriately qualified. CSWF members will maintain eligibility by completing annual Continuing Education (CEU) requirements and ensuring annual maintenance fees are paid on time per credentialing agencies' policies. CSWF members are responsible for tracking their CEUs and maintenance fee status, and ensuring they submit vouchers to the USN Certification Funding program Navy Credentialing Opportunities On-Line (Navy COOL) (www.cool.navy.mil) via command ISSM. Navy COOL will fund initial certification exams and annual maintenance fees. Navy COOL does not fund training, study prep materials, memberships, or other non-exam fees.

d. Supervisors will ensure civilian CSWF members develop an Individual Development Plan (IDP) to identify planned educational opportunities and courses they will complete to meet training and CEU requirements. IDP will be created and stored in Total Workforce Management System (TWMS) IDP module by civilian CSWF members and sent to supervisors for review and approval. Supervisors will ensure members are on track with training requirements throughout the year, and report status to COMNAVRESFOR CSWF-PM quarterly.

(1) CSWF members will:

(a) Earn and maintain appropriate credentials from the cyber-IT/CSWF qualification matrix (described in SECNAV M-5239.2) associated with the specialty area and level commensurate with the scope of major assigned duties for the position to which you are assigned.

(b) Participate in a continuous learning program as described in reference (u). A minimum of 20 hours of cyber-IT/CSWF related continuous learning annually documented in a current individual development plan.

(c) Uniformed CSWF personnel will remain part of the CSWF regardless of whether they are currently assigned to a CSWF position. Civilian personnel are considered part of the CSWF when assigned to a CSWF position. CSWF personnel may be identified in the following ways:

(d) A DON CSWF code and/or DoD function is part of their personnel record in a military personnel system or in Defense Civilian Personnel Data System (DCPDS).

(e) An identified military code such as Military Occupation Specialty (MOS), Navy Enlisted Code (NEC), Subspecialty Code (SSC), or Additional Qualification Designator (AQD). They are listed as a member of the CSWF with the appropriate DoN CSWF code in the DON/Navy/Marine Corps authoritative personnel and readiness databases. Expected participants include Government Civilians (2200 series), and/or those performing duties as described in reference (u) Military enlisted (Information Technology Specialist), or other ratings performing duties as described in reference (u) Military Officers performing duties as described in SECNAV M-5239.2.

(f) Cyber IT and CSWF personnel training and qualification compliance will be monitored by the cyber-IT and CSWF-PM. COs will assign unqualified military and civilian personnel to a supervised status for qualification/requalification or remove unqualified personnel from their cyber-IT and CSWF position while requalification is completed. Those who fail to requalify will be permanently removed from the cyber-IT and CSWF. In addition to removal from cybersecurity positions, failure to maintain required qualifications will result in counseling and proper documentation by the cyber-IT and CSWF-PM and chain of command.

12. User Training. To access DON Information Systems, users must complete annual Cyber Security Awareness training annually, at minimum. Commands are authorized to add PII and OPSEC trainings as annual requirements. Users that do not complete these annual requirements to meet DoD and DoN guidelines each fiscal year will have their account disabled. More information can be obtained in reference (x).

13. Continuity of Operations Plan (COOP). COMNAVRESFOR will verify functionality of the COMNAVRESFOR IT Continuity of Operations Plan (COOP) by exercising the COOP annually as required by reference (h). COOP dates will be advertised for command planning purposes.

a. Upon completion of the annual exercise or actual COOP, all commands are required to validate their site content for access and functionality.

b. Reserve ECH 3-4 commands N6s will notify all NAVRESCEN leadership, and N6 personnel when COMNAVRESFOR is implementing its COOP, whether during COOP-related exercises, or an actual real-life scenario in which COOP would be implemented. This will ensure situational awareness of potentially degraded services from higher Echelons.

14. Outlook Web Access (OWA). Access to NMCI's Outlook Web Access (OWA) unclassified official e-mail using personally owned and other non-DoD computers is authorized provided Commanders and users adhere to the procedures in the acceptable use of DON IT memorandum located on the Navy Reserve Homeport N6 page.

15. Common Access Card (CAC) Readers. CAC readers are considered consumables that can be purchased by each echelon's Supply department (N4), subject to the funding availability.

16. Peripherals.

a. Headsets and Webcams are authorized for purchase per reference (y) provided they are NMCI/General Services Administration (GSA) contract and Trade Agreements Act (TAA) compliant. Webcams may be authorized to provide distanced training in cases where live demonstration is required. Use of built-in laptop cams should be used to comply with this policy where possible.

b. Webcams in secure spaces must comply with the "Memorandum for Senior Pentagon Leadership Commanders of the Combatant Commands Defense Agency and DoD Field Activity Directors, Subject: Collaboration Peripherals in Secure Spaces" dated 4 June 2021.

APPENDIX A

ACRONYMS AND DEFINITIONS

The following is a list of the current acronyms and definitions referenced throughout this instruction.

1. Anti-Virus Software. Software designed to prevent, detect and remove malware, including but not limited to computer viruses, computer worms, Trojan Horses, spyware, and adware.

2. Authority to Operate. An Authority to Operate (ATO) is the formal approval (accreditation) to operate a system, which is granted by the DAA. Once granted, an ATO is good for three years.

3. Common Access Card (CAC). A U.S. DoD issued smart card for multifactor authentication to networks and information systems. CACs are issued as standard identification for Active-Duty military personnel, Reserve personnel, civilian employees, non-DoD government employees, state employees of the National Guard and eligible contractor personnel. In addition to its use as an identification card, a CAC is required for access to government buildings and computer networks.

4. CAC Reader. A physical device used as a communications medium between the CAC and a host (e.g., a computer, a point-of-sale terminal) or a mobile phone.

5. Media Access Control Address. A unique identifier assigned to network interfaces and devices for communications on the physical network segment.

6. Office of the Designated Approving Authority (DAA). Provides centralized management and de-centralized execution of the Certification and Accreditation (C&A) process for all DoD information systems. The Office of the DAA is accountable for timely, consistent policy implementation and C&A determinations with the DoD.

7. Pass Phrase. A sequence of words or other text used to control access to a computer system, program or data. A pass phrase is similar to a password in usage but is generally longer for added security.

8. Personally Identifiable Information. Refers to information that can be used to uniquely identify, contact or locate an individual, or can be used with other sources to uniquely identify a single individual. This includes name, birth dates, Social Security Numbers, rank, address, phone number, etc.

9. Physical Security. Describes measures designed to deny access to unauthorized personnel (including attackers, or even accidental intruders) from physically accessing a building, facility, resource or stored information.

10. Wi-Fi. A branded standard for wirelessly connecting electronic devices. A Wi-Fi device, such as a personal computer, can connect to the internet via a wireless network access point.

APPENDIX B

NAVY RESERVE FORCE NAVY RESERVE CENTER WI-FI USER DEVICE INITIAL SET-UP CHECKLIST

1. Before initially being approved for connecting to the EIS Network, the following actions will be completed:

   a. Complete Cybersecurity, PII, and OPSEC (as required) annual training requirements.

   b. Sign and date EIS User Agreement form.

   c. Enable an up-to-date anti-virus software.

   d. Enable firewall.

   e. Receive pass phrase from designated command ISSM/ISSO or applicable CSWF personnel.

2. After initial approval for EIS access is granted, users are responsible for maintaining virus updates and ensuring the firewall is enabled prior to network access per the User Agreement.

APPENDIX C

PROCESS FOR COMMAND TRUSTED AGENTS TO STAND UP OR REQUEST SIPR ACCOUNT/TOKENS

1. TA Program Requirements.

a. A minimum of two Registration Support TAs must be fully qualified and designated at all times per command. To be fully qualified, the three requirements, below must be completed. See enclosure (1) "Step-by-Step Process for Command Trusted Agents to stand up or request SIPR Account/Tokens". PIN Reset TAs are not required per NCMS Norfolk Trusted Agent SOP v5 01 May 23. PIN Reset TAs are not able to request CRI from the LRA team nor order SIPR tokens from NIWC LANT. COMNAVRESFOR LRA provides pin resets to ensure all commands have enough manning to meet the minimum of two Registration Support TAs.

(1) NCMS Trusted Agent training certificate. Contact one of the following POCs to schedule an online training: NCMS PKI Team San Diego, email: NCMS_SDAS_PKI@us.navy.mil, COMM: 1 (619) 524-0043 or NCMS PKI Team Norfolk, Email: NCMS_NRFK_PKI_AUDITORS@NAVY.MIL, COMM: 1 (757) 341-8100.

(2) Trusted Agent Designation Letter. Example located at: https://private.navyreserve.navy.mil/COMNAVRESFORCOM/N-Codes/N6/N64/_layouts/15/DocIdRedir.aspx?ID=CCW4DY7PX73K-958535215-593

(3) Trusted Agent NSS PKI Acknowledgement of Responsibilities Form. Form located at: https://private.navyreserve.navy.mil/COMNAVRESFORCOM/N-Codes/N6/N64/_layouts/15/DocIdRedir.aspx?ID=CCW4DY7PX73K-958535215-595

b. Prospective TA(s) are required to scan and email the following documentation via encrypted email to the COMNAVRESFORCOM LRA Team (cnrf_issm@us.navy.mil). The member(s) will upload, and file all required documents onto the COMNAVRESFORCOM LRA's SharePoint page.

(1) TA Designation Letter (signed by current CO) naming convention is the following: Command Name, Designation Letter, date of signature (DDMMMYY).

(2) NCMS TA training certificate and NSS PKI Trusted Agent Acknowledgement of Responsibilities form naming convention is the following: Rate/Rank, Last Name, First Name, topic (ex., NCMS TA Training Certificate, NSS PKI Acknowledgement form).

c. After the Command TAs are qualified, 90m CIW software program is required to be installed on the Commands SIPR machine.

2. Roles & Responsibilities.

a. The Supported Command (Active Component Command). To support Reserve Force member SIPR access, requirements need to be communicated from supported Commands, via their designated Reserve Program Director (RPD), to echelon V NRAs and the identified Reserve Force member. It is the Supported Command RPDs responsibility to include these requirements in official orders (ADSW, RECALL, AT, or ADT) and to ensure members have fulfilled those requirements prior to order

execution. This includes Reserve members who typically would not require SIPR access but do require access to support an exercise (AT) or mobilization requirement. For IDT billets requiring SIPR accounts for performance of duties, supported command RPDs must list SIPR requirements in the billet description in Career Management System - Interactive Detailing (CMS-ID) for enlisted billets, or list them in the Supported Command comments in Reserve Force Manpower Tools (RFMT) for officer billets.

(1) The Reserve member will complete the required documents (SAAR-N, DD-2842, Cyber Awareness training, and PII training) prior to contacting their NRC (TRUIC) to request SIPR Account and SIPR Token support. Email communication will be via encrypted email unless otherwise stated. See enclosure (1) "Step-by-Step Process for Reserve Sailors to request a SIPR Account and Token issuance".

b. Echelon 4 Trusted Agent (TA).

(1) If the reserve ECH 3-4 subordinate command cannot provide support to the Reserve member, reserve ECH 3-4 commands will take ownership and provide assistance to the Reserve member by completing the TA steps.

(2) If neither the reserve ECH 3-4 commands nor the NRC can provide support to the Reserve member, supported command LRA/TA qualified commands are encouraged to assist if able and with prior coordination.

c. Echelon 3 NRC (TRUIC) Trusted Agent (TA).

(1) Responsible for all Crossed Assigned out reserve Sailors SIPR Account and SIPR Token creation, activation, and reenablement.

(2) SIPR Account. Reviews the Member's System Authorization Access Request (SAAR) and training certifications.

(a) Determines whether there are any issues with the SAAR or training certifications. If there are issues, then the member and the Unit resolve the issues. If there are no issues, then the TAs will submit the Move Add Change (MAC) request to NMCI in coordination with target issuance date for SIPRNET account creation.

(b) Reviews the Member's DD-2842

(c) Submits MAC request to NMCI once SAAR is complete for SIPRNET account creation.

(d) Once account is created, the NRC TA will submit token request to CNRF LRA.

(3) SIPR Token.

(a) Manage blank, formatted, and enrolled tokens; reorder new tokens when stock is low.

(b) Request CRI data for the purpose of SIPR token enrollment.

(c) Submit token revocation requests and coordinate return process for failed tokens.

(d) Maintain a log of requested CRIs and enrolled SIPR tokens.

(e) The NRC TAs will communicate and schedule an appointment with the member to pick up the newly assigned SIPR token.

(f) The TA is to issue the token to the member and instruct the member to log in to their SIPRNET account. Logging in requires and IAM and calling NMCI.

(g) Once logged in the member is required to associate the token to the account immediately. The token is only valid for 30 days after the date of issuance. After token association the process ends.

STEP-BY-STEP PROCESS FOR RESERVE SAILORS TO REQUEST A SIPR ACCOUNT AND TOKEN ISSUANCE

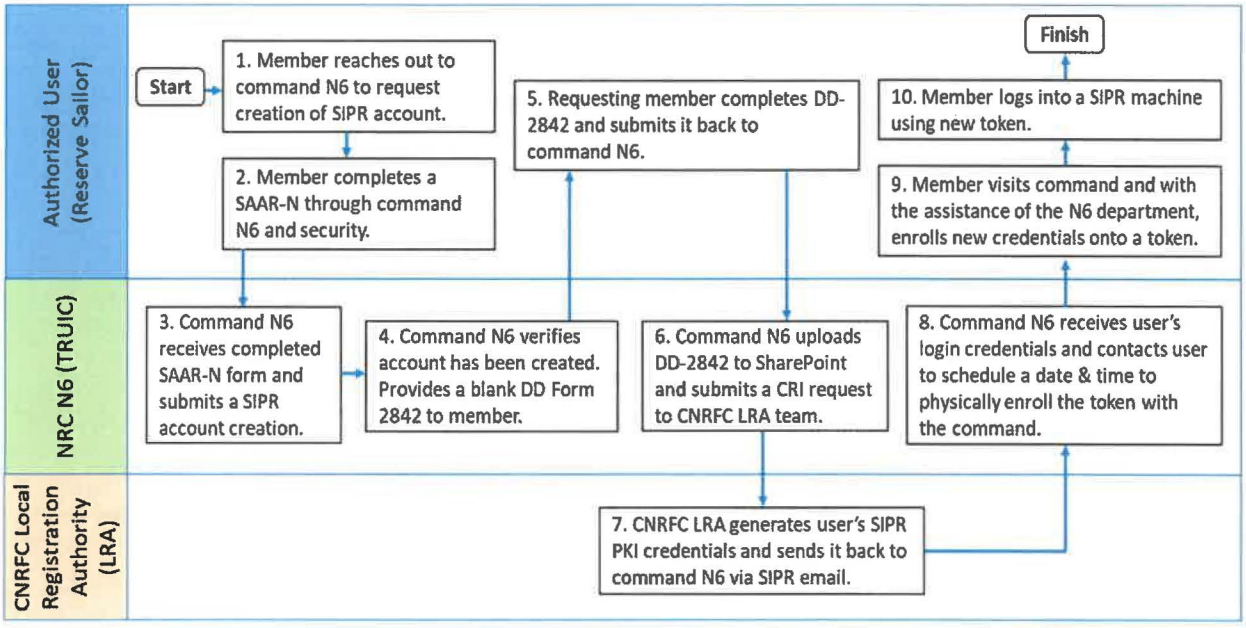

Figure (1)

STEP-BY-STEP PROCESS FOR COMMAND TRUSTED AGENTS TO STAND UP OR REQUEST SIPR ACCOUNT/TOKENS

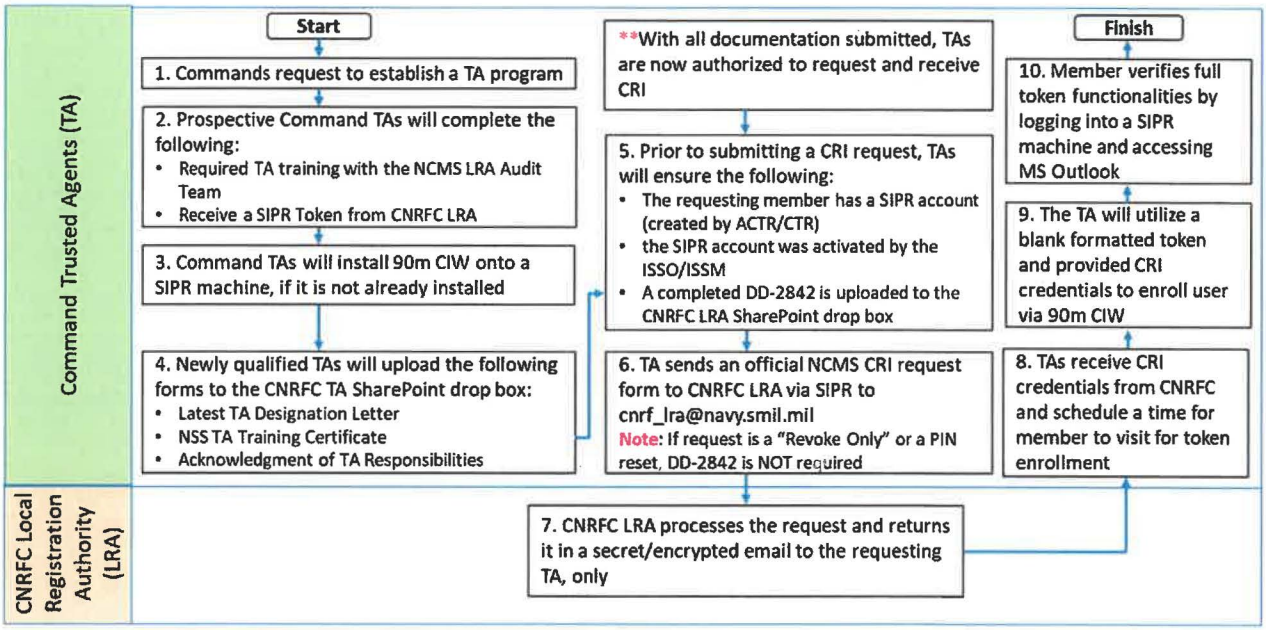

Figure (2)