HOW TO UNLOCK / CREATE AN NMCI EMAIL ACCOUNT

Is your account Locked or Deleted?

NIPR Reservist accounts will be **DISABLED/DELETED** with a policy of **60/180 days** respectively. If you have been out to sea for a long period of time, your account has most likely been deleted. **Before creating a drop-box submission with the requirements below,** you may be able to save some time by calling the NMCI Help Desk.

NMCI Help Desk Contact Information: 1-866-843-6624

During your call, follow these steps through the voice options:

1) Press 1- for UNCLASS email
2) Press 1- for NMCI
3) Press 2- for NMCI
4) Press 2- for Other
5) Once speaking to an NMCI representative, they will ask for your NMCI Email address. Once they locate your account, request whether or not the account has been locked versus disabled.

Locked: Send an email to **CNRFC_N14_ISSO@navy.mil** so we can unlock your account.

1) Request to ISSO Should Include:
    a. Navy Email Address
    b. Indicate that your email has been Locked and you have verified it with the NMCI Help Desk on Date **/**/****
    c. NOTE: SAAR-N form and annual trainings are **NOT** needed. These are only required to rebuild deleted accounts as indicated below.

Disabled/Deleted: To Create your NMCI email account you will need **3 things:**
1) DOD Annual Cyber Awareness Training (certificate required from *current* FY)
2) DOD Annual Privacy Training (certificate required from *current* FY)
3) SAAR-N form (Blank form on SSO N14 SharePoint page under Training Dept, NMCI Email)
    - SAAR form needs to be downloaded and opened locally on computer; web browser view does not work
    - Once opened, you may need to click "enable all features" to view/edit the form
    - **Follow directions below on how to fill out form!**
        i. E-sign form with CAC

Training Websites to Use
- Navy eLearning: https://learning.nel.navy.mil/ELIAASv2p/
- TWMS: https://twms.dc3n.navy.mil/my.policy
- JKO: https://jkodirect.jten.mil/Atlas2/page/login/Login.jsf?utm_source=mnp%20public

<u>Once you have completed ALL items above:</u>
- Submit them to the Ops/Training Dropbox under the sub-code: Email unlocks

<u>Things to note:</u>
- Requests normally take up to 3-4 weeks for your email account to be built
- <mark>First time login on new accounts will need to be done at a NOSC (specifically on an NMCI computer)</mark>
- Once email account is created, you **MUST** complete your first time login within **30 days** otherwise it will lock again and then delete.
  - After you've logged in and your email is up and running:
    - For Reservists, email accounts lock at 60 days and delete at 180 days

LASTLY! Have you been Flanked?

Have you been Flanked? If you are having trouble logging into Outlook Web Access or you are receiving an error that shows :(something went wrong: we could not find a mailbox for this user. You may have been flanked. Try logging into flank speed by using the following steps:

1) In browser type 'portal.apps.navy' or google flank speed log in

2) Click portal.apps.navy link on page

3) Enter email 'fathom@us.navy.mil

4) Click CAC login and your email should be firstname.MI.lastname.mil@us.navy.mil (flank speed email)

5) Click Outlook App on left column

If you can get into the Outlook App, YOU HAVE BEEN FLANKED. If you cannot or it does not show the app, YOU HAVE NOT. If you are still having trouble after following these steps, please reach out to the N14 ISSO. CNRFC_N14_ISSO@navy.mil.

PLEASE NOTE: If you have been fully Flanked, you will longer need your NMCI account. NMCI accounts are being phased out and you will only need to access your Flank Speed account through the portal and Outlook App on the left column. There is no login requirement for Flank Speed. "

How to fill out the SAAR-N

SYSTEM AUTHORIZATION ACCESS REQUEST NAVY (SAAR-N)

PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 10450, Public Law 99-474, the Computer Fraud and Abuse Act; and System of Records Notice: NM0500-2 Program Management and Locator System.

PRINCIPAL PURPOSE: To record user identification for the purpose of verifying the identities of individuals requesting access to Department of Defense (DOD) systems and information.

ROUTINE USES: The collection of data is used by Navy Personnel Supervisors/Managers, Administration Office, Security Managers, Information Assurance Managers, and System Administration with a need to know.

DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

Date →

TYPE OF REQUEST: ☒ INITIAL ☐ MODIFICATION ☐ DEACTIVATE ☐ USER ID _____	DATE (DDMMMYYYY):

SYSTEM NAME (Platform or Application): NMCI	LOCATION (Physical Location of System): NORFOLK, VA

PART I (To be completed by Requester)

Your Name →

1. NAME (Last, First, Middle Initial):	2. ORGANIZATION: COMNAVRESFOR

3. OFFICE SYMBOL/DEPARTMENT: N14 SSRG UIC 2525M	4. PHONE (DSN and Commercial): DSN: COM: 1-800-535-2580

Your Navy Email →

Grade /Rank →

5. OFFICIAL E-MAIL ADDRESS:	6. JOB TITLE AND GRADE/RANK: SSO/ O-

7. OFFICIAL MAILING ADDRESS: 1915 Forrestal Drive, Norfolk VA 23508	8. CITIZENSHIP: ☒ US ☐ FN ☐ LN ☐ Other _____	9. DESIGNATION OF PERSON: ☒ MILITARY ☐ CIVILIAN ☐ CONTRACTOR

Check box and type in Date →

Date Completed (on certificate) →

10. INFORMATION ASSURANCE (IA) AWARENESS TRAINING REQUIREMENTS (Complete as required for user or functional level access.)
☐ I have completed Annual IA Awareness Training.   DATE (DDMMMYYYY): _____

PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR (If an individual is a contractor - provide company name, contract number, and date of contract expiration in Block 14a).

11. JUSTIFICATION FOR ACCESS: ACCESS TO GOVERNMENT IT SYSTEMS IS REQUIRED TO EXECUTE ASSIGNED DUTIES
DOD ID #

Type your DOD ID # It is found on Back of CAC →

12. TYPE OF ACCESS REQUIRED: ☒ AUTHORIZED ☐ PRIVILEGED	12a. If Block 12 is checked "Privileged", user must sign a Privileged Access Agreement Form.	DATE SIGNED (DDMMMYYYY):

13. USER REQUIRES ACCESS TO: ☒ UNCLASSIFIED ☐ CLASSIFIED (Specify Category): _____ ☐ OTHER: _____

Ensure box is checked →

Leave as is. →

Leave as is. →

14. VERIFICATION OF NEED TO KNOW: I certify that this user requires access as requested. ☒	14a. ACCESS EXPIRATION DATE (Contractors must specify Company Name, Contract Number, Expiration Date):

15. SUPERVISOR'S ORGANIZATION/DEPARTMENT: COMNAVRESFOR N14	15a. SUPERVISOR'S E-MAIL ADDRESS:	15b. PHONE NUMBER: 800-535-2580
16. SUPERVISOR'S NAME (Print Name):	16a. SUPERVISOR'S SIGNATURE	16b. DATE (DDMMMYYYY):
17. SIGNATURE OF INFORMATION OWNER/OPR:	17a. PHONE NUMBER:	17b. DATE (DDMMMYYYY):
18. SIGNATURE OF IAM OR APPOINTEE:	19. ORGANIZATION/DEPARTMENT:	20. PHONE NUMBER:	21. DATE (DDMMMYYYY):

(Block 22 Cont)

I further understand that, when using Navy IT resources, I shall not:
- Auto-forward any e-mail from a Navy account to commercial e-mail account (e.g. .com).
- Bypass, stress, or test IA or Computer Network Defense (CND) mechanisms (e.g., Firewalls, Content Filters, Proxy Servers, Anti-Virus Programs).
- 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 the Local IA Authority (i.e., person responsible for the overall implementation of IA at the command level).
- Use personally owned hardware, software, shareware, or public domain software without written authorization from the Local IA Authority.
- Upload/download executable files (e.g., exe, .com, .vbs, or .bat) onto Navy IT resources without the written 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.
- Use Navy IT resources in a way that would reflect adversely on the Navy. Such uses include 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 PII, and other uses that are incompatible with public service.
- Place data onto Navy IT resources possessing insufficient security controls to protect that data at the required classification (e.g., Secret onto Unclassified).

23. NAME *(Last, First, Middle Initial)*:	24. USER SIGNATURE:	25. DATE SIGNED *(DDMMMYYYY)*:

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

26. TYPE OF INVESTIGATION:	26a. DATE OF INVESTIGATION *(DDMMMYYYY)*:

26b. CLEARANCE LEVEL: SECRET	26c. IT LEVEL DESIGNATION ☐ LEVEL I ☒ LEVEL II ☐ LEVEL III

27. VERIFIED BY *(Print name)*:	28. SECURITY MANAGER TELEPHONE NUMBER: 757-322-2598	29. SECURITY MANAGER SIGNATURE:	30. DATE *(DDMMMYYYY)*:

PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION

31. TITLE:	31a. SYSTEM:	31b. ACCOUNT CODE:
	31c. DOMAIN:	
	31d. SERVER:	
	31e. APPLICATION:	
	31f. DATASETS:	
	31g. DIRECTORIES:	
	31h. FILES:	
32. DATE PROCESSED *(DDMMMYYYY)*:	32a. PROCESSED BY:	32b. DATE *(DDMMMYYYY)*:
33. DATE REVALIDATED *(DDMMMYYYY)*:	33a. REVALIDATED BY:	33b. DATE *(DDMMMYYYY)*: