RESET FORM

The information on this form is requested under the authority of DoD Instruction 8520.03, Identity Authentication for Information Systems, to grant or deny access to CNIC Fleet and Family Readiness (FFR) Business Systems and networks and manage access control. This form is to be used for new user accounts, additions or deletions of specific access, reactivations and terminations of access to network and applications.

Instructions for CNIC FFR Systems Access Request Form

1. Complete the access request form, obtain supervisor's approval, and submit via email.

2. For all requests, **SECTIONS 1, 2, 9** and **11, MUST BE COMPLETED**. Sign section 11 and obtain supervisor's approval and signature in section 11. In addition,
   - For CYMS access complete section 3.
   - For Kronos access check the box in section 4.
   - For FFR SAP Portal, SAP ERP, or SAP HR access complete section 5.

   When assigning Roles click the drop-down button of the required role and select "ADD or DELETE" to remove and existing role from a User.

   - For FFR Navy Single Sign On portal access complete section 6.
     - *SSO is exempt from Section 9.*
   - For CNIC N9 GovCloud access complete section 7.
     - CNIC N9 GovCloud includes: JIRA, Confluence, Media Manager
     - *CNIC N9 GovCloud is exempt from Section 9.*
   - Privileged Users complete sections 8 and 12.
   - If requesting access to a system that is not listed, note it in section 10.
   - For Risk Assessment access complete section 8.1.

   ***IF YOU CURRENTLY HAVE A CITRIX ID, LIST IT IN SECTION 2.**

3. Submit signed forms by emailing to support@cnicffr.org; If the form only pertains to SAP HR (Section 5.3) email to mill_mwr_saphrhd.fct@navy.mil.
   - SAP users continue to submit via your authorization coordinator

Idle accounts will be disabled after DoD-designated periods of inactivity

RESET FORM

PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 10450, Public Law 99-474, the Computer Fraud and Abuse Act; and Systems of Records Notice: NM0500-2 Program Management and Locator System and NM01700-1, DON General Morale, Welfare, and Recreation Records.

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.

1. USER INFORMATION (TO BE COMPLETED BY REQUESTOR)

GIVEN NAME	PHONE (DSN)	PHONE (COMMERCIAL)	EMAIL	
JOB ROLE	DEPARTMENT		PROGRAM	N CODE
REGION	INSTALLATION		SITE / CENTER	BLDG #

2. REQUEST TYPE

INITIAL REQUEST ☐	MODIFICATION ☐	REACTIVATE ☐	DEACTIVATE ☐
PRIVILEGED ACCESS ☐	If "Privileged Access" is checked, the user must sign section 12, the Privileged Access Agreement		
VALIDITY DATES FROM: TO: If end date is known	CITRIX USER ID If the request is an account modification or deactivation, please provide the current Citrix User ID above.		

3. CYMS

If you are replacing someone, please provide that person's name and CYMS ID~	CYMS ROLE:	☐ DIRECTOR	☐ REGIONAL ACCOUNTING	☐ STAFF
		☐ FRONT DESK	☐ RESOURCE & REFERRAL	☐ TRAINING & CURRICULUM

4. KRONOS

KRONOS ☐

5. SAP

5.1 SAP ERP

ROLE				RETAIL ROLE	
General Office User	AR Invoice Tech	Display Sensitive Fields		Retail Account Tech	Retail MM Release Code (provide code below)
AP Check Writer	Asset Management Tech	GL Account Supervisor		Retail Inventory Tech	
AP Invoice Tech	Bank Tech	GL Account Tech		Retail MM Contracting Officer	
AP Local Payments Tech	Budget Tech	MM Contracting Officer		Retail MM Site Manager	Below list requested Company/Release Codes:
AP Supervisor	Check Printer	MM Tech		Retail MM Tech	
AP Vendor Tech	Check Reversal	Report Printer		Retail MM Warehouse Manager	
AR Customer Tech	CO Supervisor				

5.2 FFR SAP PORTAL AND BW

ACCESS LEVEL	GOLF WEB APP	DASHBOARD	FINANCIAL REPORTING	PROGRAM REPORTING

5.3 SAP HR

MASTER DATA INPUT		DISPLAY ONLY W/ INFO TYPES		ADHOC QUERY		
ACTIVITY MANAGER		ORG UNIT (REQUIRED FOR ACTIVITY MANAGER)				
REGION		☐ MWR	☐ NGIS	☐ WFS	☐ CYP	☐ OTHER (SPECIFY)
INSTALLATIONS		☐ ALL	☐ OTHER (SPECIFY)			

6. NAVY SINGLE SIGN ON (SSO)

CYP	FITNESS	MARKETING	MOVIES	MTP	TRAINING
LIST JOB ROLES					

7. CNIC N9 GOVCLOUD

7.1 JIRA

ACCESS LEVEL	DISPLAY ONLY	PROJECT MANAGER	PROJECT TEAM	LIST PROJECTS

7.2 CONFLUENCE

ACCESS LEVEL	DISPLAY ONLY	PROJECT TEAM	PMO	LIST PROJECTS

7.3 MEDIA MANAGER

ACCESS LEVEL	LIST ROLE

8. NETWORK APPLICATIONS

MANAGE ENGINE DESKTOP CENTRAL	CRIMS	AD MANAGER PLUS	
SUPPORT CENTER	ORION	MOVE COMPUTERS	RESET PASSWORDS
SHAREPOINT (LIST FOLDERS)		MOVE USERS	UNLOCK USERS

8.1 RISK ASSESSMENT

ACCESS LEVEL

9. COMPLETION OF BACKGROUND INVESTIGATION AND ANNUAL TRAINING

Completion Date of Cyber Awareness Training	Date Background Investigation completed by Security Manager
Completion Date of Operational Security Training	Security Manager Name

10. SPECIAL INSTRUCTIONS / ADDITIONAL DETAILS

11. USER AGREEMENT - STANDARD MANDATORY NOTICE & CONSENT PROVISION:

signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

- 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:

- 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.
- At any time, the U.S. Government may inspect and seize data stored on this information system.
- 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.
- 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.

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:

- 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.

11. USER AGREEMENT - STANDARD MANDATORY NOTICE & CONSENT PROVISION:

- 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.
- 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.
- 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.

USER RESPONSIBILITIES:

- I understand that to ensure the confidentiality, integrity, availability, and security of Navy Information Technology (IT) resources and information, when using those resources, I shall:
- Safeguard information and information systems from unauthorized or inadvertent modification, disclosure, destruction, or misuse.
- Protect Controlled Unclassified Information (CUI), to include Personally Identifiable Information (PII), and classified information to prevent unauthorized access, compromise, tampering, or exploitation of the information.
- Protect authenticators (e.g., Password and Personal Identification Numbers (PIN)) required for logon authentication at the same classification as the highest classification of the information accessed.
- Protect authentication tokens (e.g., Common Access Card (CAC), Alternate Logon Token (ALT), Personal Identity Verification (PIV), National Security Systems (NSS) tokens, etc.) at all times. Authentication tokens shall not be left unattended at any time unless properly secured.
- Virus-check all information, programs, and other files prior to uploading onto any Navy IT resource.
- Report all security incidents including PII breaches immediately in accordance with applicable procedures.
- Access only that data, control information, software, hardware, and firmware for which I am authorized access, have a need-to-know, and have the appropriate security clearance. Assume only those roles and privileges for which I am authorized.
- Observe all policies and procedures governing the secure operation and authorized use of the information system.
- Digitally sign and encrypt e-mail in accordance with current policies.
- Employ sound operations security measures in accordance with DOD, DON, service and command directives.
- 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).
  - Share my password or authentication tokens

11. APPROVAL INFORMATION

11.1 REQUESTOR APPROVAL

NAME (LAST, FIRST, MIDDLE INITIAL)	SIGNATURE	DATE
APPROVERS NAME	SIGNATURE	DATE

APPROVERS EMAIL

11.2 IAM OR APPOINTEE APPROVAL

SIGNATURE OF IAM OR APPOINTEE (HQ Internal Use Only)	ORGANIZATION / DEPARTMENT	PHONE NUMBER	DATE

By signing, I acknowledge that I have read, understood, and agree to the User Terms and Conditions.

12. PRIVILEGED ACCESS AGREEMENT – FFR NAF ENTERPRISE NETWORK PRIVILEGED USER AGREEMENT

INFORMATION SYSTEM PRIVILEGED ACCESS AGREEMENT AND ACKNOWLEDGEMENT OF RESPONSIBILITIES

1. I understand there are two DoD Information Systems (IS), classified (SIPRNet) and unclassified (NIPRNet). I understand that the Navy Fleet and Family Readiness (FFR) Non-Appropriated Fund (NAF) Enterprise Network is an unclassified, private, commercial network operating the systems of the FFR Accounting and Information Management System (AIMS), and that I have the necessary clearance for privileged access to the FFR NAF Network. I will not introduce or process data for the Information System (IS) which I have not been specifically authorized to handle.
2. I understand the need to protect all passwords and other authenticators at the highest level of data they secure. I will not share any password(s), account(s), or other authenticators with other coworkers or other personnel not authorized to access the FFR NAF Network. As a privileged user, I understand the need to protect the root password and/or authenticators at the highest level of data it secures. I will not share the root password and/or authenticators with coworkers who are not authorized FFR NAF Network privileged access.
3. I understand that passwords for all accounts with elevated privileges (Service Accounts, System Administrators, Backup Operators, etc.) must comply with Department of Defense requirements for privileged user password complexity. Personnel with elevated privileges will comply with FFR NAF Network two-factor authentication requirements for remote network access.
4. I understand that I am responsible for all actions taken under my account(s). I will not attempt to gain access to data, FFR NAF Network devices, systems, or any interconnected systems to which I do not have authorized access.
5. I understand my responsibility to appropriately protect and label all output generated under my account (including printed materials, magnetic tapes, floppy disks, and downloaded hard disk files).
6. I will immediately report any indication of computer network intrusion, unexplained degradation, or interruption of network services, or the actual or possible compromise of data or file access controls to the appropriate FFR NAF Network Information Assurance (IA) personnel, security personnel, or senior management. I will not install, modify, or remove any hardware or software without written permission and approval from FFR NAF Network IA (N946) or the FFR NAF Network Configuration Control Board.
7. I will not install any unauthorized software (e.g., games, entertainment software, etc) or hardware (e.g., sniffers).
8. I will not add any users' names to the Domain Admins, Local Administrator, or Power Users group without the prior approval and direction of FFR NAF Network IA or the Configuration Control Board.
9. I will not introduce any unauthorized code, Trojan horse programs, malicious code, or viruses into the FFR NAF Network wide or local area networks.
10. I understand that I am prohibited from the following while browsing the web:
    a) Introducing Classified and/or Unclassified Controlled Information (UCI) into an unclassified system or environment.
    b) Accessing, storing, processing, displaying, distributing, transmitting, or viewing material that is abusive, harassing, defamatory, vulgar, pornographic, profane, or racist; that promotes hate crimes, or is subversive or objectionable by nature, including material encouraging criminal activity, or violation of local, state, federal, national, or international law.
    c) Storing, accessing, processing, or distributing Classified, Proprietary, UCI, For Official Use Only (FOUO) or Privacy Act protected information in violation of established security and information release policies.
    d) Obtaining, installing, copying, pasting, transferring, or using software or other materials obtained in violation of the appropriate vendor's patent, copyright, trade secret, or license agreement.
    e) Knowingly writing, coding, compiling, storing, transmitting, or transferring malicious software code, to include viruses, logic bombs, worms, and macro viruses.
    f) Promoting partisan political activity.
    g) Disseminating materials unrelated to an established command religious program.
    h) Using the system for personal financial gain such as advertising or solicitation of services or sale of personal property (e.g., eBay), or stock trading (i.e., issuing buy, hold and/or sell directions to an online broker).
    i) Fundraising activities, either for profit or non-profit, unless the activity is specifically approved by the command (e.g., Command social event fund raisers, charitable fund raisers, etc., without approval).
    j) Gambling, wagering, or placing of any bets.
    k) Writing, forwarding, or participating in chain letters.
    l) Posting personal home pages.
11. I understand that personal encryption of electronic communications is strictly prohibited and can result in the immediate termination of access.
12. I understand that if I am in doubt as to any of my roles or responsibilities I will contact FFR NAF Network management personnel for clarification.
13. I understand that all information processed on the FFR NAF Network is subject to monitoring. This includes e-mail and browsing the web. I will not attempt to circumvent any monitoring, auditing or logging mechanisms deployed on the FFR NAF network.
14. I will not allow any user who is not cleared access to the network or any other connected system without prior approval or specific guidance from FFR NAF Network IA Management.
15. I will use the special access or privileges granted to me only to perform authorized tasks or mission related functions.
16. I will not use any FFR owned information systems to violate software copyright by making illegal copies of software.
17. I will use my PRIVILEGED USER account only for official administrative actions. I will not use my account for day-to-day network communications.
18. I understand that failure to comply with the above requirements will be reported and may lead to the following actions:
    a) Chain of command revocation of FFR NAF Network privileged access and/or user privileges
    b) Counseling
    c) Adverse actions under the Uniform Code of Military Justice and/or criminal prosecution
    d) Disciplinary action, discharge or loss of employment
19. I will obtain and maintain required certification(s), competency, and training to retain privileged system access.

USER NAME	SIGNATURE	DATE

By signing, I acknowledge that I have read, understood, and agree to the Privileged Access Agreement.