NCTS FE System Authorization and Access Request (SAAR) Policy

ONE-Net Far East Cybersecurity Policy

OUTSIDE CONTINENTAL UNITED STATES NAVY ENTERPRISE NETWORK
NAVAL COMPUTER & TELECOMMUNICATIONS STATION FAR EAST
Document Version: 1.0
Date: 28 Feb 2024

Revision History

Version #	Date	Owner	Revised By	Revision Description
1.0	28 FEB 2024	ISSM	SM	Initial issuance; significant changes from SAAR-N policy

Approved By:

CARTER.ERIC.M.1246685785

Digitally signed by CARTER.ERIC.M.1246685785
Date: 2024.02.28 09:37:31 +09'00'

Eric M. Carter
NCTS FE Regional ISSM

Annual Review 1:

_____

Annual Review 2:

_____

1. PURPOSE

This policy outlines the security requirements and conditions necessary for account creation, maintenance, lockout and deactivation for the Outside Continental United States Navy Enterprise Network (ONE-Net) user accounts under Naval Computer and Telecommunications Stations, Far East (NCTS FE) purview. This document was developed in accordance with Executive Order 10450, 9397; Public Law 99-474, The Computer Fraud and Abuse Act, applicable DoD/DoN policy and guidance, and ONE-Net Enterprise policy and guidance.

NCTS FE complies with and adheres to the cited references. This document focuses on ONE-Net Far East requirements for user account access controls and ensures that requisite documentation is consistent with the system's overall sensitivity, operational strategy, acquisition plan, and life-cycle status.

2. APPLICABILITY

This policy applies to all components, subsystems, and interfaces that comprise each ONE-Net Far East system configuration. It applies to all NCTS FE ONE-Net user groups including but not limited to end-users, operators, managers, and administrators including government civilian, military, and contractor personnel who use, operate, manage, maintain, or administer NCTS FE ONE-Net computer systems that process, store, or transmit information. This document is applicable to the ONE-Net sites identified below.

Applicable	Location	Code	Applicable	Location	Code
☐	ONE-Net Enterprise	ON	☒	Sasebo, Japan	SA
☒	Yokosuka, Japan	YO	☒	Singapore	SP
☒	Atsugi, Japan	AT	☒	Iwakuni, Japan	IW
☒	Diego Garcia, BIOT	DG	☐	Manama, Bahrain	BA
☒	Guam	GU	☐	Naples, Italy	NA
☒	Chinhae, Korea	KO	☐	Rota, Spain	RO
☒	Misawa, Japan	MI	☐	Sigonella, Italy	SI
☒	Okinawa, Japan	OK	☐	Souda Bay, Greece	SB

3. REFERENCES

The following references inform this policy:

(a) DOD 5400.11-R Dated 14 May 2007
(b) DOD M-5200.02, Change 1 Dated 29 Oct 2020
(c) DODI 5200.48 Dated 6 Mar 2020
(d) DODI 8500.01, Change 1 Dated 7 Oct 2019
(e) SECNAV 5239.2 Dated Jun 2016
(f) SECNAV 5510.30C Dated 24 Jan 2020
(g) SECNAV 3070.2a Dated 9 May 2019
(h) SECNAV M5210.1, Change 3, Records Management Program Dated Sep 2019

(i) DON CIO Acceptable use of DON IT Policy Dated 25 Feb 2020
(j) NAVADMIN 259-23 Dated 3 Nov 2023
(k) OPNAV INSTRUCTION 5239.1E Dated 17 Nov 2023
(l) ONE-Net Information Bulletin (OIB) 3H Dated 27 Jun 2019
(m) Federal Investigative Standards Crosswalk Job Aid dated 15 Apr 2020
(n) NIST SP 800-37 Rev. 2 Dated Dec 2018
(o) DON CIO Memorandum for Distribution IT Level Designation on DD Form 2875 System Authorization Access Request Dated 8 September 2020
(p) OIB 2H SAAR Dated 7 Dec 2023

4. BACKGROUND

This policy replaces prior policies using the deprecated SAAR-N form as of the date signed.

5. POLICY:

A ONE-Net account is a privilege, and is not the inherent right of any user. See Appendix 1, SAAR Guide for required handling of the SAAR or the DD Form 2875.

The Navy user agreement must be signed and including as part of the SAAR submission package to the ESD.

6. RESCISSIONS

NCTS FE System Authorization Access Request-Navy (SAAR-N) Policy version 2.7 dated 10 August 2023.

7. VALIDITY

This policy remains in effect until cancelled or superseded. This document is reviewed annually and will be re-issued every three years.

Appendices:
APPENDIX 1: SAAR Guide

Appendix 1: SAAR Guide

1. SAAR

1.1 Submission Process

Note: All accounts will be Cryptographic Logon (CLO) enforced upon creation.

All SAARs will be electronically signed and submitted digitally, unless prior approval is obtained from the NCTS FE ONE-Net Regional Information System Security Manager (ISSM). In order for handwritten forms to be processed, they must be completed entirely in pen and ink and be legible; otherwise, the request will be rejected. Pen and ink submissions must also include the user's Electronic Data Interchange Personal Identifier (EDIPI) /DoD ID Number (located on the back of user's Common Access Card (CAC)).

Sample SAARs for various access request types are located here.

I. All submissions except requests to deactivate accounts must include a fully, accurately completed SAAR with appropriate signatures.

Account creation documents must come from properly designated personnel. To be designated as a recognized ITR for ONE-Net submissions coordinate with your local LNSC to become an ITR for ONE-Net.

NOTE: The Navy user agreement is not included within the SAAR. Signing and uploading the Navy user agreement separately as part of the SAAR submission package is a requirement for successful processing and account provisioning.

a. Submissions for NCTS FE personnel, signed by NCTS FE ISSM/Information System Security Officer (ISSO):

i. Official documentation proving completion of and compliance with current mandated Cyber Awareness Challenge (i.e. certificate of completion, TWMS, or FLTMPS), and Operations Security (OPSEC).

ii. SIPRNET access requests further require:

1. Documentation proving completion of and compliance with annual mandated Derivative Classification Training; and

2. Completed NATO Brief with briefing officer's signature.

b. Submissions for external command personnel, signed by external command ISSM:

i. Proof of training is not required. Required training is verified as part of the check by the user's command ISSM. Through reciprocity, ISSM signature validates that users have met Cybersecurity training requirements for access.

ii. SIPRNET access requests further require:

1. Documentation of Derivative Classification Training and NATO brief are not required, however, completion dates must be documented on the SAAR in block 13. Through reciprocity, Security Manager and ISSM signatures validate that users have met applicable requirements for access, including Derivative Classification training and completion of NATO brief.

   Note: NATO briefs are provided by the user's Command Security Manager (CSM), not ONE-Net.

II. IAW ref j, all of the following apply: SAARs providing access to any Navy network, system, or application that have been approved by other Navy commands and organizations will be honored under reciprocity. This will be applied at the same or lower classification level and need-to-know status. If a user is requesting for an account at a higher classification level than what was annotated on the approved SAAR, then a new SAAR package will be required to be completed.

a. Modifications to move accounts within the Navy and reactivate disabled accounts due to inactivity no longer require a new SAAR form to be submitted. The command ISSM, ISSO, or Information System Coordinator (ISC) (note: on ONE-Net, the ISC role is filled by the Information Technology Representative (ITR)) will request account movement or reactivation after validating the current SAAR form and completion of mandatory training.

b. Users that have a change of personnel status (i.e. MIL to CIV) will be required to submit new SAAR package.

c. For reservists who are also employed within the Navy as contractors or civilians, one SAAR is required for each personnel category.

III. Privileged Access Account requests further require the following:

a. NCTS FE ISSM or designee must complete blocks 19, 19a, 19c and sign block 19b of the Privileged Access SAARs;

b. Fully, accurately completed Privileged Access Agreement (PAA) Form SECNAV 5239/1. NCTS FE ISSM or designee and Cyber Security Workforce Manager (NCTS FE Training and Readiness) must sign off on the PAA; and

c. Privileged User Cybersecurity Responsibilities (PUCR) training completion certificate.

IV. Functional Account requests (creation/modification) further require the following:

a. SAAR must be populated with the account custodian's information and identify the requested functional account name in block 13;

b. Functional Account Custodian Designation Letter; and

c. Functional Account Custodian Agreement.

V. Resource Mailbox requests further require the following:

a. SAAR must be populated with the account custodian's information and identify the requested resource mailbox name in block 13;

b. Resource Mailbox Designation Letter; and

c. Resource Mailbox Custodian Agreement.

VI. Naval Nuclear Propulsion Information (NNPI) account requests further require the following:

a. NNPI User Statement of Acceptance and Acknowledgement of Responsibility completion date is required in block 13.

Be advised, account requests lacking the required documentation will not be processed until corrected and in compliance with this policy.

2. Amplifying Guidance

2.1 SAAR Header

NOTE: Do not enter DOB, SSN, and similar personal data not requested or required for the SAAR. Entering this data would cause a change in handling requirements to comply with relevant regulations and laws. If any information of this nature is included in the form, it will be rejected and the form will need to be resubmitted.

I. Type of Request

a. Initial: Indicates that the user is new to the ONE-Net or Legacy network.
b. Modification: Used when an existing account needs to be modified for reasons including but not limited to: extensions, name changes, personnel status, or reinstatements.
c. Deactivation: Used when the user no longer requires access.
d. USER ID: Leave blank for initial, the office provisioning the account will fill in with the proper naming convention. If it is a modification or deactivation, enter the users existing USER ID.

II. Date: Date the request is filled out.

III. System Name: Name of the system to which access is being requested, for example: "ONE-Net".

IV. Location: Location of the Command (Region, Base, Command, and Building Number).

2.2 PART I

I. Block 1, Name: The user's last name, first name and middle initial. Only full legal names are allowed, and must match the official government-issued ID. Nicknames are NOT authorized.

II. Block 2, Organization: Enter the name of the user's current organization (i.e. DISA, NCTS FE, Government Agency or Commercial Firm).

III. Block 3, Office Symbol/Department: Enter user office symbol or department; must be completed.

IV. Block 4, Phone: The Defense Switching Network (DSN) phone number of the user. If DSN is unavailable, indicate commercial number; must be completed.

V. Block 5, Official E-mail Address: On initial requests, this shall be left blank. For account modifications and deactivations the users official e-mail address must be entered. ***Ensure @us.navy.mil address is provided for this block in the event of a modification or deactivation.**

VI. Block 6, Job Title/Grade/Rank: Civilian Job Title (i.e., System Analyst, GS-11), Military rank (i.e., CAPT, USN; PO1, USN; CPO, USN etc.) or "CTR" if user is a contractor. Identification by rate is not allowed.

VII. Block 7, Official Mailing Address: The user's command mailing address. This is required.

VIII. Block 8, Citizenship

a. US: Checked when the user is a US citizen.

b. Foreign National (FN): Reserved for users who are not US citizens, including Local Nationals (LNs). If this is used, the appropriate Geopolitical Entities, Names, and Codes (GENC) standard code must be indicated in block 8. Standard codes can be found here: https://www.state.gov/s/inr/rls/4250.htm or here: Registers of the Geopolitical Entities, Names, and Codes Registry (nga.mil).

   LNs will check the FN box and indicate their citizenship in Block 21, OPTIONAL INFORMATION in the format: LN/Citizenship or FN/Citizenship.

   EX: LN/Japan
   EX: FN/Australia

c. Other: Reserved for anomalies that do not fall into the above categories.

   Personnel that fall in this category will also indicate their citizenship(s) in Block 21, OPTIONAL INFORMATION, in the manner prescribed above in section VIII. b.

IX. Block 9, Designation of Person: Military is used for military personnel; Civilian is used for DoD civilian personnel (USCS) or respective country government worker (FN or LN). Contractor is used for contracted personnel.

X. Block 10, IA Training and Awareness Certification Requirements: The box must be checked. The training date on this line must correspond to the date on the Cyber Awareness Challenge training certificate.

2.3 PART II

I. Blocks 11-12: User Signature and date signed; must be completed.

II. Block 13, Justification for Access: A justification statement must be entered in this block.

In support of OIB-3H requirements for account management, requestors are required to indicate in this block if they are Reservists. This requirement is without regard to branch of service or type of reservist (i.e. SELRES or IRR). *The accepted format is "Reservist:" and then "Yes" or "No" as applicable.*

Non-Navy military members requesting access to ONE-Net must specify which branch of service they are in.

If access to SIPRNET is requested, proof of a signed NATO brief and Derivative Classification Certificate must be annotated with dates of completion in Block 13.

III. Block 14, Type of Access Required: Separate SAARs must be submitted for authorized and privileged accounts.

a. Authorized: This is selected to indicate that the user is authorized to access the network.

b. Privileged: Privileged accounts are only provisioned to authorized personnel. This is selected when a user is designated as an administrator on the subject system. All privileged accounts require approval from the NCTS FE ISSM. Privileged account requests must be accompanied by a Privileged Access Agreement & Acknowledgement (PAA) (SECNAV 5239/1), which must be signed the NCTS FE ISSM and NCTS FE Command Cyber Security Work Force (CSWF) Program Manager (PM). The NCTS FE CSWF PM retains copies of all PAAs and ensures proper credentials are maintained in order to retain privileged access.

IV. Block 15, User Requires Access To: All applicable checkboxes should be checked.

a. Access to NIPRNET: Check Unclassified.

b. Access to SIPRNET: Check Classified, Specify Category: SIPRNET.

c. Access to NNPI: Check Classified, Specify Category: NNPI

i. Note: A single SAAR can be submitted for a NIPR account and a SIPR NNPI account. ONE-Net only supports NNPI on SIPR.

V. Block 16, Verification of Need to Know: This box must be checked.

VI. Block 16a, Access Expiration Date: Complete as follows, using YYYYMMDD format:

a. Military, US Civil Service (Civilian - GS, GG, etc.), FN or LN Government Workers: No expiration date required except for temporary access of 1 year or less.

b. Contractors: Must specify Company Name, Contract Number and Expiration Date.

VII. Blocks 17, Supervisor's Name: The supervisor prints his/her name to indicate that the above information has been verified and that access is required.

VIII. Blocks 17a-b, Supervisors Email Address and Phone Number: Must be completed.

IX. Block 17c, Supervisor's Organization/Department: Must be completed.

X. Blocks 17d-e, Supervisor's Signature and Date: Must be completed. ***Note: for ONE-Net Far East, these blocks must be signed by military or US Civil Service.***

XI. Block 18, Signature of Information Owner/OPR: Information Owner signature. This block will be signed by an ISSM, ISSO, IT Representative (ITR), or designated Information Owner for requested access at the user's command. ***Note: this block must be signed by military or US Civil Service. Foreign Nationals and contractors are specifically prohibited from signing as Information Owner.***

XII. Blocks 18a and c, Information Owner Phone Number and Date: Must be completed.

XIII. Blocks 19, 19a, and 19c: ISSO or appointee's organization, phone number, and date signed; must be completed.

XIV. Block 19b, Signature of Information System Security Officer (ISSO) or Appointee: This is the signature of the ISSO (or appointee) at user's command. This is the person responsible for ensuring all access requirements are met and recurring mandatory training is completed. This shall be the last block signed prior to account creation.

NOTE: Account creation documents will only be accepted from properly designated personnel. All properly designated personnel must be listed on the Navy-wide ISSM/ISSO list located here. Instructions on how to add / remove personnel from the ISSM/ISSO can be found here.

XV. Controlled Unclassified Information (CUI) and Personally Identifiable Information (PII)

When filled in, 2875 contains CUI and PII and must be protected in accordance with all applicable laws, regulations, and policies, as outlined on the DoN CIO website located at http://www.doncio.navy.mil.

Upon changing the DD 2875 header and footer from "UNCLASSIFIED" to CUI, a CUI control block will appear on the right hand side of the page 1 footer. The block should be filled in with the following:

Controlled by: <Command> CUI Category: PERS/CONTROLLED Distribution/Dissemination Control: FEDCON POC: <Submitter's name> <Submitters phone number>	**EXAMPLE:** Controlled by: NCTS FE CUI Category: PERS/CONTROLLED Distribution/Dissemination Control: FEDCON POC: Joe Navy, 315-123-4567

XVI. Block 20, Name: Enter name in Last, First, Middle Initial format.

XVII. Block 21, Optional Information: Additional information that will facilitate provisioning of access, to include anything listed in this policy.

2.4 PART III

Note: The user's servicing Security Manager validates the background investigation/clearance information. This part is required to be filled in by the user's servicing Security Manager for ALL (Classified and Unclassified) account requests. The only repository for verifying investigations and security clearance eligibilities for civilian, contractor and military personnel is Defense Information System for Security (DISS). Local National and Foreign National investigations are verified through their servicing Human Resource Office (HRO).

I. Block 22, Type of Investigation: **T3/T3R/T5/T5R** Use "GOJ" for MLC employees, "ROK" for Korean Local Nationals, "NBI" for Philippine Nationals, "GUK" for Diego Garcia Local Nationals, and "ROS" for Singaporean Nationals. All other instances, check with the servicing Security Manager. For submitted investigations where eligibility is pending, the type of investigation submitted (as listed above) will be entered.

II. Block 22a, Investigation Date: For submitted investigations where eligibility is pending, open, scheduled or in progress, the date of investigation should state "pending". Otherwise, enter the date of last investigation.

III. Block 22b, Continuous Evaluation (CE) Enrollment Date: Date enrolled in CE in prescribed format (YYYYMMDD) will be entered.

IV. Block 22c, Access Level:

(1) The user's current security clearance access level (Interim Secret, Top Secret, SCI, etc.). N/A is not acceptable for a security clearance eligibility level; a minimum clearance eligibility level of Interim Secret is required if user is requesting access to the Classified ONE-Net system. Clearance must be within scope (five years for Secret and above).

(2) In the event of an open investigation, network access is still possible. Individuals with prior investigations can utilize that information in block 22 as long as DISS reflects the open investigation and the investigation submitted date is reflected in block 22a.

(3) Local Nationals and Foreign Nationals do not undergo the Department of Defense investigative process due to their locale and inaccessibility in DoD automated systems. As a result, local nationals undergo a background check through their local government as stipulated in the Status of Forces Agreement (SOFA). While local nationals do not normally access classified systems (outside of the foreign disclosure program), they can access unclassified systems using the local government background investigation. The local government agreement will determine when (if ever) the background investigations will expire. For purposes of block 22c, the clearance level will be "Favorable". For block 22, (Type of Investigation), use the convention stated above for Local Nationals.

(4) A favorable background investigation (T1 or other) must have been completed if the user is requesting access to the Unclassified ONE-Net system.

(5) If the result of an investigation or background check is UNFAVORABLE, then the individual will not be granted access to NIPR/SIPR information; this is reciprocated across to sensitive information, equipment, and systems. The following security clearance eligibility determinations render a subject's investigation unfavorable: ie. Revoked, Terminated for Cause; Denied. Per DoD M-5200.02, all positions require a favorably adjudicated investigation regardless of access.

(6) Upon receipt of derogatory information, the NCTS Commanding Officer can suspend or remove network access regardless of the individual's billet. Individuals with a Denied or Revoked final security determination who have exhausted due process rights must obtain a "favorable" CAF position of trust suitability determination for continued access. Security Managers can obtain a final adjudication status by submitting a CSR via DISS.

(7) U.S. Military and USCS civilians with less than 12 months of remaining service time can use the current investigation regardless of the date.

Table 1 Investigation Types and Possible Outcomes

Investigation	Possible
T1(R)/T2(R)	Favorable, Unfavorable
T3(R)	None, No Determination, Specified Security level (Secret, Confidential), Revoked
T5(R)	None, No Determination, Specified Security level (Secret, TS, Confidential), Revoked
GOJ/ROK/NBI/ROS/GUK	Favorable, Unfavorable

V. Block 23, Verified By: The Security Manager or designee prints his/her name to indicate verification of security access and favorable investigation.

VI. Blocks 24-26 Security Manager Phone Number, Signature, and Date: must be completed.

2.5 PART IV

Completed by Authorized Staff preparing account information. This area of the SAAR is reserved for NASM, and is beyond the scope of this document. No information should be entered here.

3. Retention Period

The complete original account creation package will be retained in accordance with reference (b) for a minimum of one year post account deletion. Electronic copies of all completed SAAR packages are maintained at NCTS FE HQ, however, all Commands are required to retain local copies of their completed SAAR packages, with the exception of Part IV.

4. Account Deactivation

The Command's ISSM/ISSO or ITR must inform the ONE-Net ESD when a user account is no longer required by submitting a "Deactivation" SAAR (only blocks 1-9 and 14-19c are required).

5. Account Disablement

Each user is bound to adhere to the Navy Acceptable Use Policy (AUP) and various DoD/DoN policies, to include the consequences of violating those policies. A ONE-Net account is a privilege and not a right of any user. As such, access may be denied or suspended for conduct deemed inappropriate, disruptive, or dangerous to the network. When a user violates a provision of the Navy AUP, the violator's account(s) are immediately disabled to ensure preservation of data to support any continued investigation and to limit additional damage.

All incidents will be handled in accordance with the NCTS FE Cyber Incident Response Policy.