



SAAR-N Completion Guide

FOR OFFICIAL USE ONLY

NCTS FE IA

ONE-NET Information Assurance

1. SAAR-N Submission

- All submissions except requests to deactivate accounts must include a fully completed SAAR-N and a copy of the IA Certificate that indicates that the user has completed annual Information Assurance training. The name of the user issued the certificate must match field 1 on the SAAR-N.
- NATO brief required to be submitted with SIPRNET requests.
- All SAAR-Ns will be digitally signed and submitted electronically. Scanned and handwritten SAAR-N request will not be accepted.

All authorized NIPRNET Accounts will be CLO enabled upon creation.

2. Header

- **Type of Request**
 - **Initial** indicates that the user is new to the ONE-NET or Legacy network
 - **Modification** is used when an existing account needs to be modified
 - Change of Command
 - Change of Region
 - Military to Civilian/Government worker
 - Name change.
 - **Deactivate** is used when the user no longer requires access to ONE-NET
- **User ID** On initial requests this shall be left blank. For account modifications and deactivations the user's official username / EDIPI number shall be entered.
- **Date.** The date that the request is submitted
- **System Name**
 - ONE-NET
- **Location.** Location of the command (Region, Base, and Building Number)

3. Part I

- **Block 1. Name.** The user's last name, first name and middle initial. Only full legal names are allowed. Nicknames are NOT authorized. The name listed here must match the signed IA training certificate and the user's CAC.
- **Block 2. Organization.** This is reserved for the name of the user's command.
- **Block 3. Office Symbol/Department.** User's office symbol or department name.
- **Block 4. Phone.** DSN and Commercial (Prefix 81 Japan, 65 Singapore, 82 South Korea 1671 Guam, 246 Diego Garcia + commercial number).
- **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 shall be entered.
- **Block 6. Job Title/Grade/Rank.** Civilian Job Title (i.e., System Analyst, GS-11), Military rank (Commanding Officer /CAPT, USN; Logistical Supply Analyst / PO1, USN; etc.) or "CTR" if user is a contractor. Identification by Rate is not allowed.
- **Block 7. Official Mailing Address.** The user's command mailing address.
- **Block 8. Citizenship**
 - **US.** Checked when the user is a US citizen

FOR OFFICIAL USE ONLY

NCTS FE IA

ONE-NET Information Assurance

- **FN.** Reserved for users who are citizens of countries other than the US. If this is used, the appropriate Federal Information Processing Standard (FIPS) 10-4 standard code must be indicated. If the TASO or user has generated this form electronically, this code needs to be written inside box 9. Some of the commonly used codes in the Far East are below.
- **LN and Others.** are not options

Country	FIPS Code
Korea	KS
Malaysia	MY
Japan	JA
Philippines	RP
Singapore	SN

The rest can be found on the state department website.
<http://www.state.gov/s/inr/rls/4250.htm>

- **Block 9. Designation of Person.** Military is used for military personnel; Civilian is used for DoD civilian personnel. Contractor is used for contracted personnel including the MLC population.
- **Block 10. IA Training and Awareness.** The box must be checked. The training date on this line must correspond to the date on the attached IA Certificate.
 - The Department of Defense Cyber Awareness training is the only accepted version. ONE-Net will not accept the Federal version of the Cyber Awareness training.
 - Training must not be older than the latest Cyber Security and Information System Security Awareness training NAVADMIN

4. PART II

- Endorsement of access by Information Owner or Government Sponsor.
- Contract personnel cannot endorse Part II.
- **Block 11. Justification for Access.** A justification statement must to be entered in this block.
- **Block 12. Type of Access Required.** Separate SAAR-Ns need to be submitted for authorized, privileged, and NNPI accounts
 - **Authorized.** This is selected to indicate that the user is authorized to access the network.
 - **Privileged.** Separate SAAR-N is required for privileged access due to the requirement that the FE IAM signature is required prior to approval. This is selected when a user is designated as an administrator on the ONE-NET or Legacy network. All requests for Privileged accounts must include a signed OCONUS Navy Enterprise Network (ONE-NET) information

FOR OFFICIAL USE ONLY

NCTS FE IA

ONE-NET Information Assurance

System (IS) Privileged Access Agreement in addition to the IA Cyber Awareness training certificate and NATO brief (SIPRNET).

- **NNPI.** Separate SAAR-N is required for NNPI access due to the requirement that the FE IAM signature is required prior to approval. All requests for NNPI accounts must include a signed NNPI User Statement of Acceptance and Acknowledgement of Responsibility form.
- **Block 13. User Requires Access To.** All applicable boxes should be checked.
- **Block 14. Verification of Need To Know.** This box must be checked.
- **Block 14a. Access Expiration Date.**
 - This should be completed as follows:
 - **Military.** Projected Rotation Date (PRD) or End of Active Obligated Service (EAOS), whichever comes first.
 - **US Civil Service (aka GS workers).** 3 years from date of initial request or rotation date.
 - **Contractors.** Must specify Company Name, Contract Number and expiration Date.
- **Block 15. Supervisor's Organization/Department.** Supervisor's organization and department
- **Block 15a. Supervisor's e-mail address.** Supervisor's e-mail address
- **Block 15b. Phone Number.** Supervisor's telephone number
- **Block 16. Supervisor's Name.** The supervisor or representative prints his/her name to indicate that the above information has been verified and that access is required.
- **Block 16a. Supervisor's Signature.** Supervisor's digital signature
- **Block 16b. Date.** Date supervisor signs the form
- **Block 17. Signature of Information Owner/OPR.** IT Representative's digital signature
- **Block 17a. Phone Number.** IT Rep telephone number
- **Block 17b. Date.** The date the IT Rep/N6 signs the SAAR-N
- **Block 18. Signature of Information Assurance Officer (IAO) or Appointee.** Command IAM's representative's digital signature
- **Block 19. Organization/Department.** The organization and department
- **Block 20. Phone Number.** DSN number
- **Block 21. Date.** The date signed.
- **Block 22. User Agreement** – Standard Mandatory Notice and Consent Provision. User requesting account MUST read, understand and acknowledge his/her responsibilities once account is granted. Violation of any of these responsibilities may lead to the loss of the user account. User requesting the account needs to read Block 22.
- **Block 23. Name.** Same as Block 1
- **Block 24. User Signature.** User digitally signs acknowledging that they have read Block 22
- **Block 25. Date.** Date that block 24 is signed

FOR OFFICIAL USE ONLY

NCTS FE IA

ONE-NET Information Assurance

5. PART III

- Security Manager validates the background investigation or clearance information. This part is required to be filled in by the command security manager for all account (Classified and Unclassified). Additional information is available in the SECNAV M-5510.30 Personnel Security Program Manual.
- **Block 26. Type of Investigation** The user's last type of background investigation (e.g. GOJ, NAC, NACI, or SSBI.)
- **Block 26a. Date of Investigation.** Date of last investigation.

Block 26b. Clearance Level. The user's current security clearance level (Secret, Top Secret, SCI, etc). A minimum clearance level of Interim Secret is required if user is requesting access to the Classified ONE-NET system. A favorable background check must have been completed if the user is requesting access to the Unclassified ONE-NET system.

Investigation	Possible
NACI	Favorable, Unfavorable
NACLC (Tier 3)	None, No Determination, Specified Security level (Secret, TS, Confidential), Revoked
SSBI	None, No Determination, Specified Security level (Secret, TS, Confidential), Revoked
SBPR	None, No Determination, Specified Security level (Secret, TS), Revoked
Others	None, No Determination, Specified Security level (Secret, TS, Confidential), Revoked

N/A is not acceptable for a security clearance or eligibility determination. Must be one of the above.

Supervisors are advised to check their users' security clearance eligibility before they submit a SAAR. The following should be noted:

- 1) A security clearance eligibility is not necessary for Unclassified sensitive access but an investigation with favorable results is needed.
- 2) If the result of the investigation/background check is UNFAVORABLE, individuals will not be granted access to classified information and this is reciprocated across to sensitive information, equipment, and systems.

FOR OFFICIAL USE ONLY

NCTS FE IA

ONE-NET Information Assurance

The only area that deals with favorable or unfavorable is the National Agency Check with Inquiry (NACI) which is the minimum required investigation for first term personnel in the military (Officer & Enlisted)

For Tier 3, SSBI, SBPR, Others, they are investigations submitted for access classified information.

- **Block 26c. IT Level Designation.** The user's IT designation (Level I, Level II, or Level III) Level is identified on the user's job description, or by Human Resources. Per DOD Directive 8500.1, Level I = Privileged, Level II = Limited Privileged, sensitive information access and Level III = Non-Privileged, no sensitive information access. To be determined by the users command and inputted into JPAS by the Command Security Manager.
- **Block 27. Verified By.** The Security Manager or designated representative prints his/her name to indicate that the above clearance and investigation information has been verified.
- **Block 28. Security Manager Telephone Number.** The telephone number of the Security Manager or his/her representative.
- **Block 29. Security Manager Signature.** The Security Manager or designated representative indicates that the above clearance and investigation information has been verified.
- **Block 30. Date.** The date that the form was signed by the Security Manager or the command designated representative.

6. Part IV

- Completion by Authorized Staff Preparing Account Information. This area of the SAAR-N is reserved for NASM, and is beyond the scope of this SOP. No information should be entered here.