SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

OMB No. 0704-0630
OMB approval expires: 20250531

PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 10450; and Pu
PRINCIPAL PURPOSE(S): To record names, alidating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOT d/or paper form
ROUTINE USE(S): None.
DISCLOSURE: Disclosure of this information is information may impede, delay or prevent further processing of this request.

YELLOW- COMPLETED BY REQUESTER
PURPLE- COMPLETE BY SUPERVISOR
GREEN- COMPLETED BY C7F/N6
RED- COMPLETED BY SECURITY MANAGERS

TYPE OF REQUEST: SAAR GUIDE

☒ INITIAL ☐ MODIFICATION ☐ DEACTIVATE ☐ USERID <N/A>

DATE *(DDMMMYYYY)*: 06-Apr-2023

SYSTEM NAME *(Platform or Applications)*: ARSENAL MISSION PACKAGE (AMP)

LOCATION *(Physical Location of System)*: Far East Base: Yokosuka BLDG# 39B

PART I *(To be completed by Requester)*

1. NAME *(Last, First, Middle Initial)*: Navy, Joe S.

2. ORGANIZATION: U.S. SEVENTH FLEET (COMSEVENTHFLT)

3. OFFICE SYMBOL/DEPARTMENT *(i.e. C7F/N6 MOC SUPPORT)*: C7F/ EXERCISE Support Lead

4. PHONE *(DSN or Commercial, if known)*: DSN: (315) 241-9018 COM:

5. OFFICIAL E-MAIL ADDRESS: <NOT REQUIRED FOR INITIAL REQUESTS>

6. JOB TITLE AND GRADE/RANK *(i.e. E-7 / USN / ITC / LCPO)*: RANK: E-8 BRANCH: US Navy DCLPO

7. OFFICIAL MAILING ADDRESS
COMSEVENTHFLT
UNIT 200225 BOX 1
FPO, AP 96602

8. CITIZENSHIP NEED HELP?
☒ US ☐ FN ☐ OTHER

9. DESIGNATION OF PERSON
☒ MILITARY ☐ CIVILIAN ☐ CONTRACTOR

10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS *(Complete as required for user or functional level access.)*

☒ I have completed the ***CURRENT FY*** Annual Cyber Awareness Training. **DATE** *(DDMMMYYYY)*: 31-Oct-2022

11. USER SIGNATURE

12. DATE *(DDMMMYYYY)*: 06-Apr-2023

PART II ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR
(If individual is a contractor - provide company name, contract number, and date of contract expiration in Block 16.)

13. JUSTIFICATION FOR ACCESS
Required for 7th Fleet operational duties and responsibilities.

DoDID: 0123456789 Are you a Reservist?: No
NATO Security Brief Date *(Required for Classified Account Access)*: 31-Oct-2022
Derivative Classification Training Date *(Required for Classified Account Access)*: 31-Oct-2022 TWMS Link (CAC) Training Link (Non-CAC)

14. TYPE OF ACCESS REQUESTED *(Choose one)*
☒ AUTHORIZED ☐ PRIVILEGED *(Required for escalated privileged access. Signed PAA REQUIRED.)*

15. USER REQUIRES ACCESS TO: ☒ UNCLASSIFIED ☒ CLASSIFIED *(Specify category)* SIPRNet (SECREL Capable - US ONLY)
☐ OTHER: N/A

16. VERIFICATION OF NEED TO KNOW
☒ I certify that this user requires access as requested.

16a. ACCESS EXPIRATION DATE *(Contractors must specify Company Name, Contract Number, Expiration Date.)*
PRD (MIL/CIV): 31-Oct-2025
Contract Info (Contractors): Company Name: Contract Number: Contract Expiration:

17. SUPERVISOR'S NAME *(Print Name)*	17a. SUPERVISOR'S EMAIL ADDRESS	17b. PHONE NUMBER
Navy, Jane S. ITCM	jane.s.navy@cf.navy.mil	(315) 241-9099
17c. SUPERVISOR'S ORGANIZATION/DEPARTMENT	**17d. SUPERVISOR SIGNATURE**	**17e. DATE** *(DDMMMYYYY)*
C7F/N6		06-Apr-2023
18. INFORMATION OWNER/OPR PHONE NUMBER	**18a. INFORMATION OWNER/OPR SIGNATURE**	**18b. DATE** *(DDMMMYYYY)*
(315) 241-9018		06-Apr-2023
19. ISSO ORGANIZATION/DEPARTMENT C7F/N6 **19a. PHONE NUMBER** (315) 241-9018	**19b. ISSO OR APPOINTEE SIGNATURE**	**19c. DATE** *(DDMMMYYYY)*: 06-Apr-2023

20. NAME *(Last, First, Middle Initial)*

Navy, Joe S.

21. OPTIONAL INFORMATION

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 by the cognizant Department of the Navy (DON) Commanding Officer, and have a need-to-know, 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 a Navy 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.
• 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, 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).
• Use Navy IT resources in which I have not been specifically granted access to by the Local IA Authority. Such uses include using another user's account, or using a functional account (group account).
• Escalate privileges on any systems or services in which I am not authorized to without explicit written authorization from the Local IA Authority.

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

22. TYPE OF INVESTIGATION	22a. INVESTIGATION DATE *(DDMMMYYYY)*	22b. CONTINUOUS EVALUATION (CE) DEFERRED INVESTIGATION
TIER 3R	04-Jul-2021	No

22c. CONTINUOUS EVALUATION (CE) ENROLLMENT DATE *(DDMMMYYYY)*	22d. ACCESS LEVEL
04-Jul-2021	SECRET

23. VERIFIED BY *(Printed Name)*	24. PHONE NUMBER	25. SECURITY MANAGER SIGNATURE	26. VERIFICATION DATE *(DDMMMYYYY)*
Obvious, Captain	(315) 241-9001		06-Apr-2023

PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION

TITLE:	SYSTEM	ACCOUNT CODE
	DOMAIN	
	SERVER	
	APPLICATION	
	FILES	
	DATASETS	
DATE PROCESSED *(DDMMMYYYY)*	PROCESSED BY *(Print name and sign)*	
DATE REVALIDATED *(DDMMMYYYY)*	REVALIDATED BY *(Print name and sign)*	

INSTRUCTIONS

The prescribing document is as issued by using DoD Component.

A. PART I: The following information is provided by the user when establishing or modifying their USER ID.

(1) Name. The last name, first name, and middle initial of the user.

(2) Organization. The user's current organization (i.e. DISA, SDI, DoD and government agency or commercial firm).

(3) Office Symbol/Department. The office symbol within the current organization (i.e. SDI).

(4) Telephone Number/DSN. The Defense Switching Network (DSN) phone number of the user. If DSN is unavailable, indicate commercial number.

(5) Official E-mail Address. The user's official e-mail address.

(6) Job Title/Grade/Rank. The civilian job title (Example: Systems Analyst, GS-14, Pay Clerk, GS-5)/military rank (COL, United States Army, CMSgt, USAF) or "CONT" if user is a contractor.

(7) Official Mailing Address. The user's official mailing address.

(8) Citizenship (US, Foreign National, or Other).

(9) Designation of Person (Military, Civilian, Contractor).

(10) IA Training and Awareness Certification Requirements. User must indicate if he/she has completed the Annual Cyber Awareness Training and the date.

(11) User's Signature. User must sign the DD Form 2875 with the understanding that they are responsible and accountable for their password and access to the system(s).

(12) Date. The date that the user signs the form.

B. PART II: The information below requires the endorsement from the user's Supervisor or the Government Sponsor.

(13) Justification for Access. A brief statement is required to justify establishment of an initial USER ID. Provide appropriate information if the USER ID or access to the current USER ID is modified.

(14) Type of Access Required: Place an "X" in the appropriate box. (Authorized - Individual with normal access. Privileged - Those with privilege to amend or change system configuration, parameters, or settings.)

(15) User Requires Access To: Place an "X" in the appropriate box. Specify category.

(16) Verification of Need to Know. To verify that the user requires access as requested.

(16a) Expiration Date for Access. The user must specify expiration date if less than 1 year.

(17) Supervisor's Name (Print Name). The supervisor or representative prints his/her name to indicate that the above information has been verified and that access is required.

(17a) E-mail Address. Supervisor's e-mail address.

(17b) Phone Number. Supervisor's telephone number.

(17c) Supervisor's Organization/Department. Supervisor's organization and department.

(17d) Supervisor's Signature. Supervisor's signature is required by the endorser or his/her representative.

(17e) Date. Date the supervisor signs the form.

(18) Phone Number. Functional appointee telephone number.

(18a) Signature of Information Owner/Office of Primary Responsibility (OPR). Signature of the Information Owner or functional appointee of the office responsible for approving access to the system being requested.

(18b) Date. The date the functional appointee signs the DD Form 2875.

(19) Organization/Department. ISSO's organization and department.

(19a) Phone Number. ISSO's telephone number.

(19b) Signature of Information Systems Security Officer (ISSO) or Appointee. Signature of the ISSO or Appointee of the office responsible for approving access to the system being requested.

(19c) Date. The date the ISSO or Appointee signs the DD Form 2875.

(21) Optional Information. This item is intended to add additional information, as required.

C. PART III: Verification of Background or Clearance.

(22) Type of Investigation. The user's last type of background investigation (i.e., Tier 3, Tier 5, etc.).

(22a) Investigation Date. Date of last investigation.

(22b) Continuous Evaluation (CE) Deferred Investigation. Select yes/no to validate whether or not the user is currently enrolled for "Deferred Investigation" in the Continuous Evaluation (CE) program.

(22c) Continuous Evaluation Enrollment Date. Date of CE enrollment. Leave blank if user is not enrolled in CE.

(22d) Access Level. The access level granted to the user by the sponsoring agency/service (i.e. Secret, Top Secret, etc.). Access level refers to the access determination made on the basis of the user's individual need for access to classified information to perform official duties; a determination separate from the user's eligibility determination.

(23) Verified By. The Security Manager or representative prints his/her name to indicate that the above clearance and investigation information has been verified.

(24) Phone Number. Security Manager's telephone number.

(25) Security Manager Signature. The Security Manager or his/her representative indicates that the above clearance and investigation information has been verified.

(26) Verification Date. Date the Security Manager performed the background investigation and clearance information verification.

D. PART IV: This information is site specific and existing blocks can be used to collect account-specific information. This information will specifically identify the access required by the user.

E. DISPOSITION OF FORM:

TRANSMISSION: Form may be electronically transmitted, faxed, or mailed. Adding a password to this form makes it a minimum of CONTROLLED UNCLASSIFIED INFORMATION" and must be protected as such.

FILING: Original SAAR, with original signatures in Parts I, II, and III, must be maintained on file for one year after termination of user's account. File may be maintained by the DoD or by the Customer's ISSO. Recommend file be maintained by ISSO adding the user to the system.