

USAFRICOM System Authorization Access Request (SAAR) TTP

PURPOSE: The USAFRICOM SAAR (DD Form 2875) is the required document for authorizing access for USAFRICOM staff on the Joint Enterprise Network (JEN). This document authorizes properly cleared individuals with the need-to-know access to NIPRNet and SIPRNet networks.

APPLICABILITY: This form applies to all military, DoD Civilians, Contractors and other assigned personnel requiring access to the USAFRICOM JEN.

SCOPE: This form replaces the previously used **CITS Account Creation document**. No changes to the USAFRICOM IT Use and User Agreement or (USAFRICOM AUP). This TTP describes required entries for the SAAR which when completed will enable network access without delay. **Failure to include information required in the USAFRICOM Template may result in unnecessary delays associated with account creation.**

WORKFLOW: The general workflow for this document is:

User:	Fills in Type of Request and Part 1.
Supervisor:	Fills in Part II
Security Manager:	Fills in Part II
Information Assurance Officer:	Completes Block 21 and Block 22
Account Service Desk:	Fills out Part IV.

Detailed description for filling out SAAR Form:

- A) Admin Information
  - Type of Request:
    - Initial
    - EDIPI (Input the 10 Digit number here) (see Common Access Card (CAC) backside: DoD ID. This a 10 digit number. Older CACs will have a social security number(SSN). SSN are not listed if not displayed on the User CAC.
  - Date: Date of the requesting action
  - System Name: Joint Enterprise Network
  - Location: Stuttgart (Kelley Barracks Users Only)
  -

SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)	
<b>PRIVACY ACT STATEMENT</b>	
<b>AUTHORITY:</b>	Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.
<b>PRINCIPAL PURPOSE:</b>	To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.
<b>ROUTINE USES:</b>	None.
<b>DISCLOSURE:</b>	Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.
<b>TYPE OF REQUEST</b>	
<input checked="" type="checkbox"/> INITIAL	<input type="checkbox"/> MODIFICATION <input type="checkbox"/> DEACTIVATE <input type="checkbox"/> USER ID EDIPI -- see CAC
DATE (YYYYMMDD) 20130713	
<b>SYSTEM NAME (Platform or Applications)</b> Joint Enterprise Network	
<b>LOCATION (Physical Location of System)</b> Stuttgart, Germany	
<b>PART I (To be completed by Requester)</b>	

USAFRICOM System Authorization Access Request (SAAR) TTP

B) PART I

- Block 1 - Name: Lastname, Firstname, MI
- Block 2 - Organization: USAFRICOM or SOCAF
- Block 3 - Office Symbol – Directorate/Division, Bldg and Room (example – Directorate: J622, Bldg: 3309, Room 110)
- Block 4 - Phone Number: See illustration below
- Block 5 - Official Email address: See illustration below
- Block 6 - Job Title and Grade/Rank, service and persona i.e. active/reserve/national guard:
- Block 7 - Official Mailing Address
- Block 8 - Citizenship – Non US Citizens should check “FN” and provide their country of Origin in Block 27 (see Block 27 for details). Otherwise, all US citizens should Check “US” as their citizenship.
- Block 9 - Designation of Person: Self explanatory
- Block 10 - IA Training:
  - Check block – User checks the box certifying he or she has completed the training.
  - IA training date – Date listed on the IA certificate. The date must be within one year of receiving the account.
- Block 11 – User’s Digital Signature
- Block 12 - Date: Self explanatory
- 

PART I (To be completed by Requestor)		
1. NAME (Last, First, Middle Initial) Smith, John Q		2. ORGANIZATION USAFRICOM
3. OFFICE SYMBOL/DEPARTMENT Directorate: JX/JX/JXX Bldg: 33XX Room: NNN		4. PHONE (DSN or Commercial) 314-421-XXXX
5. OFFICIAL E-MAIL ADDRESS DoD Enterprise Email or Not Applicable if none assigned		6. JOB TITLE AND GRADE/RANK Mil Rank or IT Specialist, GS13 or Contractor
7. OFFICIAL MAILING ADDRESS Unit Mailing Address		8. CITIZENSHIP <input checked="" type="checkbox"/> US <input type="checkbox"/> FN <input type="checkbox"/> OTHER
9. DESIGNATION OF PERSON <input type="checkbox"/> MILITARY <input checked="" type="checkbox"/> CIVILIAN <input type="checkbox"/> CONTRACTOR		
10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (Complete as required for user or functional level access.) <input checked="" type="checkbox"/> I have completed Annual Information Awareness Training.    DATE (YYYYMMDD)    20130712		
11. USER SIGNATURE		12. DATE (YYYYMMDD)

C) PART II

- Block 13 - Justification
  - DEROS
  - FDO Training Date
  - SIPR TOKEN Code – A for active, V for reservist, C for civilian, and E for contractor
  - Unit of assignment
  - Contractor Support
  - Exercise Participant – “Name of Exercise”
  - Other justifications as applicable
- Block 14 - Type of Access Required
- Block 15 - Users Require Access to:
- Block 16 - Verification of Need to Know:

USAFRICOM System Authorization Access Request (SAAR) TTP

- Block 17 - Access Expiration Date:
  - Military – Enter DEROS Date
  - Reservist/National Guard – Enter DEROS or End of reserve time whichever is shorter.
  - DoD Civilian – Enter DEROS/PCS Date
  - Contractor – Enter Contract end Date & Company Name (**Mandatory Entry for Contractors**)
  - Exercise Personnel – Specify the ending date of the exercise

<b>PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR</b> <i>(If individual is a contractor - provide company name, contract number, and date of contract expiration in Block 16.)</i>
<b>13. JUSTIFICATION FOR ACCESS</b> Justification Text:
1) DEROS:  2) FDO Scheduled Date: FDO Brief Completion Date (the schedule date may be listed, but no SIPR access will be granted until verification of FDO)  3) SIPR Token Code: ____  A= Active Duty, C = DoD Civilian, E = Contractor, V = Reservist, N = National Guard

Supervisor Approval :

- Block 17 - Supervisor’s Name: Lastname, Firstname, MI
- Block 18 - Supervisor’s Digital Signature: Self explanatory
- Block 19 - Date: Date of supervisor’s approval – Self explanatory
- Block 20 - Supervisor’s Organization or Department
- Block 20a - Supervisor’s NIPR Email Address
- Block 20b - Phone Number – Supervisor’s Phone Number

Information Owner (Blocks 21, 21a, 21b): **LEAVE BLANK**

Information Assurance Officer (Blocks 22, 23, 24, & 25): IA Training and USAFRICOM AUP Compliance

Option 1 – IAO completes section

Option 2 – No Signature is required when IA Training and USAFRICOM AUP Attached

17. SUPERVISOR'S NAME <i>(Print Name)</i> Supervisor's Lastname, First Name MI	18. SUPERVISOR'S SIGNATURE	19. DATE (YYYYMMDD)	
20. SUPERVISOR'S ORGANIZATION/DEPARTMENT Supervisor's J-Code and Department Title  <i>(Example - IJ622 Information Assurance)</i>	20a. SUPERVISOR'S E-MAIL ADDRESS	20b. PHONE NUMBER	
21. SIGNATURE OF INFORMATION OWNER/OPR	21a. PHONE NUMBER	21b. DATE (YYYYMMDD)	
22. SIGNATURE OF IAO OR APPOINTEE	23. ORGANIZATION/DEPARTMENT	24. PHONE NUMBER	25. DATE (YYYYMMDD)

## USAFRICOM System Authorization Access Request (SAAR) TTP

### Block 27 - Optional Field Information required in the USAFRICOM SAAR Template:

DoD ID/EDIPI: Enter 10 digit EDIPI from the User's ID Card (example – 1234567890)

Existing DoD Enterprise Email (EE): Users completely new to the DoD will not have an Enterprise Email and one will be requested. Users with an EE will enter their EE address. See example below.

- [Firstname.mi.lastname.mil@mail.mil](mailto:Firstname.mi.lastname.mil@mail.mil) – Military example
- [Firstname.mi.lastname.civ@mail.mil](mailto:Firstname.mi.lastname.civ@mail.mil) – Civilian example
- [Firstname.mi.lastname.ctr@mail.mil](mailto:Firstname.mi.lastname.ctr@mail.mil) – Contractor example

Additional Security Requirements: (If not included above)

- 1) FDO Brief Scheduled Date: ASD or Sponsor schedules this date for FDO
- 2) NATO Read-On Date: See Security Manager or Security Memo from the SSO.

Foreign National Country of Origin (If Applicable): All Non US Citizens, must enter their country of origin

SIPR Token Code: \_\_\_\_ (this code is included in creating a SIPR Token accessible account)

A= Active Duty, C = DoD Civilian, E = Contractor, V = Reservist, N = National Guard

Note: when the SIPR Token account "User Principle Name" correctly populated, the User will have the ability to access SIPR via the User's NSS SIPR PKI Token. Entry Example –

[1234567890.V@SMIL.MIL](mailto:1234567890.V@SMIL.MIL). V is for a reservist.

### Include Mandatory Statement in SAAR Template:

"This DD Form 2875 accompanied by the following completed documents and information constitutes approval by the IAO or Appointee (Block 22). The document/Information must be current in the time-frame provide.

- \* USAFRICOM IT Acceptable User / User Agreement.
- \* FDO Training Completed (No SIPRNet access shall be granted without completed FDO training).
- \* DoD Information Assurance or Cyber Challenge Certificate (Completed within 1 Year)"

**USAFRICOM System Authorization Access Request (SAAR) TTP**

26. NAME (Last, First, Middle Initial) Smith, John Q	
27. OPTIONAL INFORMATION (Additional information) ***Additional Information Required to process accounts within USAFRICOM***  Additional Security Requirements: 1) NATO Read-On Date:  Foreign National Country of Origin (If Applicable):  This DD Form 2875 accompanied by the following completed documents and information constitutes approval by the Information Owner/OPR (Block 21) and the IAO or Appointee (Block 22). The document/Information must be current in the time-frame provide.  * USAFRICOM IT Acceptable User / User Agreement. * FDO Training Completed (No SIPRNet access shall be granted without completed FDO training). * Current DoD Information Assurance or Cyber Challenge Certificate	
<b>PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION</b>	


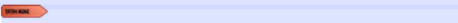
**D) PART III**

- Block 28 - Type of Investigation: SSBI – See JPAS
- Block 28a - Date of Investigation: Self Explanatory – See JPAS
- Block 28b - Clearance Level: TS/SCI, TS, SECRET, CONFIDENTIAL or NONE
- Block 28c - IT Level Designation: Most users are “Level III” or General User
- Block 29 - Verified By: Security Manager
- Block 30 - Security Manager Telephone Number: Self Explanatory
- Block 31 - Security Manager Digital Signature
- Block 32 - Date: Self Explanatory

<b>PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION</b>			
28. TYPE OF INVESTIGATION		28a. DATE OF INVESTIGATION (YYYYMMDD)	
28b. CLEARANCE LEVEL TS		28c. IT LEVEL DESIGNATION <input type="checkbox"/> LEVEL I <input type="checkbox"/> LEVEL II <input type="checkbox"/> LEVEL III	
29. VERIFIED BY (Print name) Directorate Security Manager	30. SECURITY MANAGER TELEPHONE NUMBER	31. SECURITY MANAGER SIGNATURE	32. DATE (YYYYMMDD) 20130712

USAFRICOM System Authorization Access Request (SAAR) TTP

Part IV

PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION		
TITLE:	SYSTEM	ACCOUNT CODE
	DOMAIN	
	SERVER	
	APPLICATION	
	DIRECTORIES	
	FILES	
	DATASETS	
DATE PROCESSED (YYYYMMDD)	PROCESSED BY ( <i>Print name and sign</i> ) 	DATE (YYYYMMDD)
DATE REVALIDATED (YYYYMMDD)	REVALIDATED BY ( <i>Print name and sign</i> ) 	DATE (YYYYMMDD)

DD FORM 2875 (BACK). AUG 2009

The DD Form 2875 will be retained for the duration of this account, and will be removed from accounts management upon the user's departure from USAFRICOM. File access shall be limited to operational users with a validated need to know and read only access for personnel for mission related requirements.