USSOCOM SIE NETWORK ACCOUNT REQUEST

PRIVACY ACT STATEMENT

Authority: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act

Principle Purpose: To record names and signatures for the purpose of validating the trustworthiness of individuals requesting access to USSOCOM systems and information. NOTE: Records may be maintained in electronic and/or paper form.

Disclosure: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

SECTION I - APPLICANT (Completed for Individual User)

VISITORS BADGE ACCESS GOOD UNTIL

1. TYPE OF REQUEST	2. CITIZENSHIP	3. TITLE/GRADE/RANK	4. DATE
☐ INITIAL ☐ TRANSFER *(Existing Acct)*	☒ US ☐ OTHER		

5. LAST NAME	6. FIRST NAME	7. MIDDLE INITIAL	8. DOD PIV# *(16 DIGIT)*

9. EMPLOYEE TYPE	10. COALITION COUNTRY	11. CONTRACTOR COMPANY	12. DO YOU HAVE A SIPR TOKEN?
			☐ YES ☐ NO

13. COMPONENT/TSOC	14. ORGANIZATION	15. OFFICE SYMBOL	16. COMMERCIAL DUTY PHONE/DSN
MARSOC	MRTC		16a. Commercial (10 Digit Number) 16b. DSN (10 Digit Number) 910 440

17. ORGANIZATION STREET ADDRESS	18. CITY/BASE	19. BLDG #	20. ROOM #
PSC Box 20185, Camp Lejeune NC. 28542-0185	Sneads Ferry, NC (Stone Bay)	RR-	

SECTION II - APPROVAL (Completed by Supervisor)

21. NETWORK ACCOUNT TYPE REQUIRED *(Select all that apply)*

☒ NIPRNET *(Unclass)*

☐ REL *(Foreign National)*

☒ SIPRNET *(Secret)*

22. SUPERVISOR NAME *(Print)*	23. SUPERVISOR SIGNATURE	24. SUPERVISOR PHONE
		910 440

SECTION III - CLEARANCE VALIDATION (Completed by Security Management Office)

25. DATE OF INVESTIGATION	26. CLEARANCE LEVEL	27. VERIFIED BY	28. PHONE
			910 440

29. SMO SIGNATURE

SECTION IV - ENDORSEMENT (Completed by Center/Directorate Security Manager)

30. FDO NAME *(If Applicable)*	31. FDO SIGNATURE *(If Applicable)*	32. ACCESS EXPIRATION DATE *(Contractors Only)*

33. SECURITY MANAGER NAME	34. SECURITY MANAGER SIGNATURE

BY SIGNING ABOVE, YOU AKNOWLEDGE THAT ALL THE INFORMATION WITHIN THIS FORM IS ACCURATE AND COMPLETE.

***NOTE:** Instructions for Digitally Signing the above form can be found on page 3.

***NOTE:** To enable this IMT form on Adobe, please click the yellow bar found at the top and trust this form.

USSOCOM SIE NETWORK ACCOUNT REQUEST - continued

By 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 USG-authorized use only.

- You consent to the following conditions:

-- The USG 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 USG 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 USG-authorized purpose.

-- This information system includes security measures (e.g., authentication and access controls) to protect USG interest-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 USG 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 communications or data qualifies for the protection of a privilege, or is covered by a duty 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.

--- 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 USG 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 USG 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 USG may, solely at its discretion and in accordance with DOD policy, elect to apply a privilege or other restriction on the USG'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 or 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.

I have read and understand this agreement, and my responsibilities as a network user per USSOCOM 380-3.

35. APPLICANT SIGNATURE	36. DATE

USSOCOM SIE NETWORK ACCOUNT REQUEST - continued

FORM INSTRUCTIONS

1. Type of Request - Select Initial for a new account and Transfer, if you have an account at one of the other SOF organizations and would like it transferred. If you choose Transfer, select from the drop-down menu, the Organization where you would like your account transferred from. Only the Organizations listed are available for account transfers. (Specify Organization, if form was printed and completing manually)

2. Citizenship - Enter the user's national citizenship. (abbreviated)

3. Title/Rank/Grade - Select the appropriate Title, Rank/Grade for the user. You may also type in your own value if a particular Rank is not present.

4. Date - Enter the date the form is being completed. *(MM/DD/YYYY)*

5. Last Name - Enter the user's legal last name. If Jr., Sr., III, etc... include that information after the last name.

6. First Name - Enter the user's legal first name.

7. Middle Name - Enter the first letter of the user's middle name(s). If no middle name, type NMN.

8. DOD PIV# - Enter the 16 digit PIV (Personal Identity Verification) number. This number can be found by inserting the user's CAC into a SOFNET-U CAC reader and choosing to view the certificate icon with the longer 16 digit number.

9. Employee Type - Select the appropriate employee type for the user, from the drop-down menu. (Enter one of the following, if filling out printed copy of this form: USAF, USArmy, USMC, USN, Civ, Ctr, Foreign National, USAF Reservist, US Army Reservist, USMC Reservist, USN Reservist)

10. Coalition Country - If applicable, specify Coalition Country name. (abbreviated)

11. Contractor Company - If user is a contractor specify the contractor company name.

12. Do you have a SIPR TOKEN? - Specify Yes or No, if you already have a SIPR Token.

13. Component/TSOC - Select the user's Component/TSOC from the drop-down menu. (Enter one of the following, if filling out a printed copy of this form: USSOCOM HQ, USASOC, AFSOC, MARSOC, NSW/NSWDG, JSOC, SOCAFRICA, SOCEUR, SOCCENT, SOCSOUTH, SOCNORTH

14. Organization - Enter the user's current organization.

15. Office Symbol or Unit - Enter the user's office symbol (i.e. J6-33, J2-OR, NSWG2, NSWTD2, NSWST10, 27 SOW, 24th STS, 3 SFG, MISOC, MRSG, etc…)

16. Commercial Duty Phone - Enter the user's work/office DSN phone number. If DSN is not available, then provide commercial phone number. *((XXX)-XXX-XXX)*

17. Organization Street Address - Enter the work address of the user.

18. City/Base - Enter the city or military installation name of the user's work address.

19. Bldg # - Enter the building number of the user's work address.

20. Room # - Enter the room number of the user's work address.

21. Network Account Type - Select which type(s) of account the user is requesting.

22. Supervisor Name - Enter the name of the user's supervisor.

23. Supervisor Signature - The signature of the user's supervisor (digital or ink).

24. Supervisor Phone - Enter contact number of the user's supervisor. *((XXX)-XXX-XXX)*

25. Date of Investigation - Enter the date of the user's last investigation. *(MM/DD/YYYY)*

26. Clearance Level - The security official enters the clearance level and caveats that the user holds.

27. Verified By - Enter the name of the security manager that verified the clearance level.

28. Phone - Enter the contact number for the security manager that verified the clearance level. *((XXX)-XXX-XXX)*

29. Security Management Office (SMO) Signature - The signature of the security manager that performed the verification.

30. FDO Name - Enter the name of the Foreign Disclosure Officer that validated access for the user.

31. FDO Signature - The signature of the FDO that validated access for the user.

32. Access Expiration Date - Enter the date the user's access should expire, if not renewed/updated. *(MM/DD/YYYY)*

33. Security Manager Name -Enter the name of the Security Manager (SM), Information Officer (IMO), ISSO, or IASO etc

34. Security Manager Signature -Signature of Security Manager (SM), Information Officer (IMO), ISSO, or IASO etc

35. Applicant Signature - The signature of the user/applicant.

36. Date - Enter the date the form was signed by the user. *(MM/DD/YYYY)*

Instructions for Signing a Form 12

A Form 12 can be digitally signed with a SIPRNET token or printer and routed for physical signatures.

1. Ensure that your SIPRNET token or NIPR CAC is inserted into the card reader.
2. Click the relevant signature block, a Sign Document window display with your certificate information.
3. Click the Sign button; a Save As window displays

NOTE: Digitally Sign the form requires that it be saved for routing

4. Navigate to the location where you wish to save the document.
5. Type a file name.
6. Click Save; a Windows Security window displays
7. Enter your PIN number.
8. Click OK.

The digital signature displays in the relevant signature block. The saved version of the form 12 can be emailed to the next recipient.