

SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.
PRINCIPAL PURPOSE: 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.
ROUTINE USES: None.
DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

TYPE OF REQUEST <input type="checkbox"/> INITIAL <input type="checkbox"/> MODIFICATION <input type="checkbox"/> DEACTIVATE <input type="checkbox"/> USER ID				DATE (YYYYMMDD)
SYSTEM NAME (Platform or Applications)			LOCATION (Physical Location of System)	

PART I (To be completed by Requestor)

1. NAME (Last, First, Middle Initial)		2. ORGANIZATION	
3. OFFICE SYMBOL/DEPARTMENT		4. PHONE (DSN or Commercial) DSN COMM	
5. OFFICIAL E-MAIL ADDRESS		6. JOB TITLE AND GRADE/RANK	
7. OFFICIAL MAILING ADDRESS		8. CITIZENSHIP <input type="checkbox"/> US <input type="checkbox"/> FN <input type="checkbox"/> OTHER	9. DESIGNATION OF PERSON <input type="checkbox"/> MILITARY <input type="checkbox"/> CIVILIAN <input type="checkbox"/> CONTRACTOR
10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (Complete as required for user or functional level access.) <input type="checkbox"/> I have completed Annual Information Awareness Training. DATE (YYYYMMDD) _____			
11. USER SIGNATURE			12. DATE (YYYYMMDD)

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

CCM Endorsement:

Country Code	Printed Name	Signature	Date
--------------	--------------	-----------	------

By signing in box 11 above, I am agreeing that I have read and understand the *System Rules of Behavior* and *Notice and Consent* located [here](#)

13b. Please enter a four digit numeric PIN that you will remember and will be used when requesting your password to be reset: _____

14. TYPE OF ACCESS REQUIRED:
 AUTHORIZED PRIVILEGED

15. USER REQUIRES ACCESS TO: UNCLASSIFIED CLASSIFIED (Specify category)
 OTHER _____

16. VERIFICATION OF NEED TO KNOW I certify that this user requires access as requested. <input type="checkbox"/>	16a. ACCESS EXPIRATION DATE (Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 27 if needed.)
---	--

17. SUPERVISOR'S NAME (Print Name)	18. SUPERVISOR'S SIGNATURE	19. DATE (YYYYMMDD)
------------------------------------	----------------------------	---------------------

20. SUPERVISOR'S ORGANIZATION/DEPARTMENT	20a. SUPERVISOR'S E-MAIL ADDRESS	20b. PHONE NUMBER
--	----------------------------------	-------------------

21. SIGNATURE OF INFORMATION OWNER/OPR	21a. PHONE NUMBER	21b. DATE (YYYYMMDD)
--	-------------------	----------------------

22. SIGNATURE OF IA/O OR APPOINTEE	23. ORGANIZATION/DEPARTMENT	24. PHONE NUMBER	25. DATE (YYYYMMDD)
------------------------------------	-----------------------------	------------------	---------------------

26. NAME (Last, First, Middle Initial)

27. OPTIONAL INFORMATION (Additional information)

CONTINUATION FROM BLOCK 16a (Company Name, Contract Number, Expiration Date):

Contract Number

Company Name

ADDITIONAL INFORMATION:

TODO list

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

28. TYPE OF INVESTIGATION		28a. DATE OF INVESTIGATION (YYYYMMDD)	
28b. CLEARANCE LEVEL		28c. IT LEVEL DESIGNATION <input type="checkbox"/> LEVEL I <input type="checkbox"/> LEVEL II <input type="checkbox"/> LEVEL III	
29. VERIFIED BY (Print name)	30. SECURITY MANAGER TELEPHONE NUMBER	31. SECURITY MANAGER SIGNATURE	32. DATE (YYYYMMDD)

PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION

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

SYSTEM RULES OF BEHAVIOR

United States Government systems are for authorized and official use only. All users must acknowledge and adhere to these Rules of Behavior as a condition of access to these systems.

Users shall:

- Hold a U.S. Government security clearance commensurate with the level of access granted.
- Access only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized.
- Immediately report all IA-related events and potential threats and vulnerabilities involving a DoD information system to the appropriate Information Assurance Officer (IAO).
- Protect authenticators commensurate with the classification or sensitivity of the information accessed and share authenticators or accounts only with authorized personnel. Report any compromise or suspected compromise of an authenticator to the appropriate IAO.
- Ensure that system media and output are properly marked, controlled, stored, transported, and destroyed based on classification or sensitivity and need-to-know.
- Protect terminals or workstations from unauthorized access.
- Inform the IAO when access to a particular DoD information system is no longer required.
- Observe policies and procedures governing the secure operation and authorized use of a DoD information system.
- Not unilaterally bypass, strain, or test IA mechanisms. If IA mechanisms must be bypassed, users shall coordinate the procedure with an IAO and receive written approval from the IAM.
- Not introduce or use unauthorized software, firmware, or hardware on the DoD information system. (including VOIP software)
- Not relocate or change DoD information system equipment or the network connectivity of equipment without proper authorization.
- Create only strong passwords using upper case, lower case, numeric, and special characters. Passwords will be protected against compromise and will not be shared.
- Users will not leave their CAC card or other authentication device unattended.
- Users will keep current on required information security training.
- Users will sign into the system at a minimum of every 30 days. If the user fails to sign on within this period, their account will be disabled and will require a password reset to logon. After 45 days of inactivity, the account will be deleted from the system and the user will have to submit a new system access request with current signatures.

STANDARD MANDATORY NOTICE AND CONSENT PROVISION FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS

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 U.S. Government-authorized use only.
- You may be granted access to personally identifiable information (PII) protected under The Privacy Act of 1974, as amended. PII must be protected when the system is in use and when the information is printed.

You consent to the following conditions:

- The U.S. Government 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 U.S. Government may inspect and seize data stored on this IS.
- 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 U.S. Government-authorized purpose.
- This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--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 U.S. Government 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 communication or data qualifies for the protection of a privilege, or is covered by a duty of 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 U.S. Government 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 U.S. Government 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 U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government'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 of whether the banner describes these conditions in full detail or provide a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.