

WEB PAGE AUTHORIZING SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

PRIVACY ACT STATEMENT			
Public Law 99-474, the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, authorizes collection of information. The information will be used to verify that you are an authorized user of a Government automated information system (AIS) and/or to verify your level of Government security clearance. Although disclosure of the information is voluntary, failure to provide the information may impede or prevent the processing of your "Web Page Authoring System Authorization Access Request (SAAR)". Disclosure of records or the information contained therein may be specifically disclosed outside the DoD according to the "Blanket Routine Uses" set forth at the beginning of the DISA compilation of systems of records, published annually in the Federal Register, and the disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act.			
Type of Request <input type="checkbox"/> INITIAL <input type="checkbox"/> CHANGE <input type="checkbox"/> DELETION			Date:
Part I (To be completed by user(s))			
Primary Point of Contact Information			
1. NAME (Last, Name, MI)		2. SOCIAL SECURITY NUMBER	
3. ORGANIZATION		4. OFFICE SYMBOL/DEPT	5. GRADE
6. MAILING ADDRESS (Street, Base/City, Zip Code)		7. DSN PHONE (Commercial if no DSN)	8. DSN FAX (Commercial if no DSN)
9. EMAIL ADDRESS		10. Static IP Address (Only for Self-Authoring Accounts)	
Alternate Point of Contact Information			
1. NAME (Last, Name, MI)		2. SOCIAL SECURITY NUMBER	
3. ORGANIZATION		4. OFFICE SYMBOL/DEPT	5. GRADE
6. MAILING ADDRESS (Street, Base/City, Zip Code)		7. DSN PHONE (Commercial if no DSN)	8. DSN FAX (Commercial if no DSN)
9. EMAIL ADDRESS		10. Static IP Address (Only for Self-Authoring Accounts)	
STATEMENT OF ACCOUNTABILITY			
I understand my obligation to protect my password. I assume the responsibility for data and system I am granted access to. I will not exceed my authorized			
Part II (To be completed by user's Security Manager)			
Primary User			
10. CLEARANCE LEVEL		11. TYPE IF INVESTIGATION	12. DATE OF INVESTIGATION
13. VERIFIED BY (Signature)		14. PHONE NUMBER	15. DATE
Alternate User			
16. CLEARANCE LEVEL		17. TYPE IF INVESTIGATION	18. DATE OF INVESTIGATION
19. VERIFIED BY (Signature)		20. PHONE NUMBER	21. DATE
Part III (To be completed by user's supervisor)			
22. ACCESS REQUESTED (To https://www.afms.mil Server)			
<input type="checkbox"/> SERVICE AUTHORIZING (AFMSA/SGMID POSTS DATA) <input type="checkbox"/> SELF-AUTHORIZING (USER POSTS DATA) (ENSURE BLOCKS 10 IN PART I ARE COMPLETED)			
23. ACCOUNT NAME (List what you would like your account name to be (i.e., afdental, sgmid, and so on.)			
24. JUSTIFICATION FOR ACCESS			
VERIFICATION OF NEED TO KNOW			
I certify that this user(s) requires access as requested in the performance of his/her job function.			
25. SIGNATURE OF SUPERVISOR		26. ORG/DEPT	27. PHONE NUMBER
29. SIGNATURE OF FUNCTIONAL DATA OWNER/OPR		30. ORG/DEPT	31. PHONE NUMBER
		28. DATE	32. DATE

(See Reverse for Instructions)

INSTRUCTIONS

Type of Request (Circle one that applies)

- Initial – first time request for account
- Change – change to existing account
- Deletion – removal of existing account

Part I (To be completed by both primary and alternate users)

- (1) Name: Last name, first name, and middle initial of user
- (2) Social Security Number(SSN): SSN of user
- (3) Organization: User's current organization (i.e., HQ USAF/SGD)
- (4) Office Symbol/Dept: User's office symbol within the organization listed above
- (5) Grade: User's current grade (military grade, civil service grade, or Contractor)
- (6) Mailing Address: List Street, Base/City, and Zip Code for User
- (7) DSN Phone: List DSN phone number of user (commercial if no DSN)
- (8) DSN FAX: List DSN fax number of use (commercial if no DSN)
- (9) Email Address: List valid email address for user
- (10) See end of instructions to determine IP address

Part II (To be completed by each users security manager)

- (11) Clearance Level: The user's current security clearance level (i.e., Secret, Top Secret, and so on)
- (12) Type of Investigation: User's last type of background investigation
- (13) Date of Investigation: Date of last background investigation
- (14) Verified By: The Security Manager or his representatives signature indicates that the above clearance and investigation information has been verified
- (15) Phone Number: The Security Manager's phone number
- (16) Date: The date the form as signed by the security manager or his representative
- (16-21) Same as above for alternate

Part III (Completed by User's Supervisor)

- (22) Access Requested (Circle One)
 - Service Authoring – AFMSA/SGMID posts data for user
 - Self-Authoring – User posts data
- (23) Account Name: Provide recommended account name
- (24) Justification for Access: A brief statement to justify the establishment of the account.
- (25) Signature of Supervisor: The user's supervisor must sign the request form to certify the user is authorized access
- (26) Org/Dept: Supervisor's office symbol
- (27) Phone Number: Supervisor's phone number
- (28) Date: Date signed by supervisor
- (29-3) **Will be completed by HQ AFMSA/SGMID personnel: PLEASE LEAVE BLANK**

TO DETERMINE IP ADDRESS (FOR SELF-AUTHORING ACCOUNTS ONLY) TO COMPLETE BLOCK 10 IN PART I

You can find out your IP address by going to <https://www.afms.mil/IP/>

(NOTE: If you don't have administrator privileges or your operating system is something other than Windows 2000 or NT you will need your local systems administrators help doing this)

For Windows 2000 systems

- 1) From your desktop - right click "My Network Places" and select properties
- 2) Right click "Local Area Connection" and then select properties
- 3) Highlight your TCP/IP Internet Protocol and then click properties
- 4) If the "Obtain an IP Address Automatically" is marked you have a dynamic IP address, if "Use the Following IP Address" is selected it is static and is what you want.

For NT systems

- 1) From your desktop - right click "Network Neighborhood" and select properties
- 2) Click the Protocols tab and highlight TCP/IP and then select properties
- 3) Under the IP Address tab if the "Obtain an IP Address Automatically" is marked you have a dynamic IP address, if "Use the Following IP Address" is selected it is static and is what you want.