

How to create and Submit SAAR for access to ORMA (Security Managers)

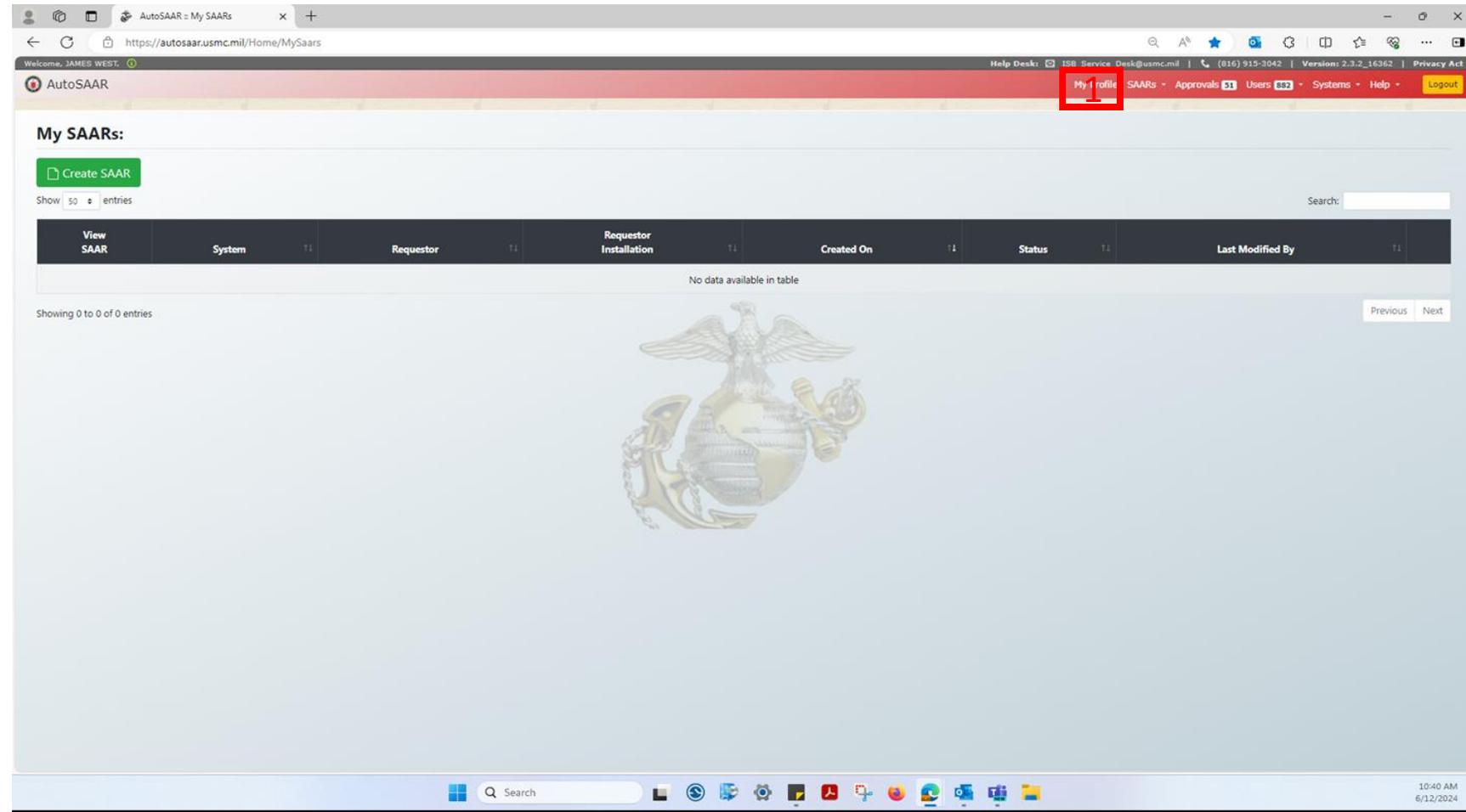
Click on the link below to open the Auto SAAR site

[AutoSAAR :: My SAARs](#)



Home Page

- 1) Please select My Profile at the top right of the page
- 2) Once there you must update your profile first see the next slide for detailed instructions.
- 3) After you have completed the profile then you need to select the training tab. See the slide after the profile for detailed instructions.



Update "My Profile"

Sub-Steps:

- 1) Select your Designation
- 2) Select "Yes" to receive email notifications
- 3) Select your Grade
- 4) Enter your work email
- 5) Enter your work phone number
- 6) Enter your job title
- 7) Enter "James West" Then select the first one you see from the drop down
- 8) Enter "Lamar Outlaw" Then select the first one you see.
- 9) Enter your work address – must match your GAL information!
- 10) Select "Marine Corps"
- 11) Select your organization
- 12) Select your installation
- 13) Select "OTHER"
- 14) This is a manual enter section please type "Security Manager"
- 15) Click "Save"

***DO NOT MOVE ON**
UNTIL YOU CLICK SAVE*

Welcome, STEVEN ELLINGTON. Help Desk: MCOMFSBServiceDesk@usmc.mil (816) 915-3042 Version: 2.1.1_14063 Privacy Act

AutoSAAR My Profile SAARs Help Logout

My Profile:

⚠ Please complete your profile to continue. Missing Field(s): Email, Installation, Office Symbol / Department

Profile Information Training Certificates

* = required field.

Designation: * 1
 Military Civilian Contractor

Citizenship: *
 US Foreign Other

Receive Email Notifications: * 2
 Yes No

Profile Datasources:
 DISS Marine Net MCTFS

Grade * 3
BWT 1-3

Display Name * STEVEN ELLINGTON

Email Address * 4
official govt. email only

Phone Number * 5

Job Title * 6
MANAGEMENT DATA SYTEMS OFFICER

Supervisor or Authorized Approver 7
Supervisor / Authorized Approver is only required to create and submit a SAAR. It does not need to be entered to

Security Manager 8
Security Manager is only required to create and submit a SAAR. It does not need to be entered to approve/deny

A Training Coordinator

Supervisor not found

Official Mailing Address

Address Type Domestic Foreign

Address Line 1 * 3280 RUSSELL RD

Address Line 2 * 9

City * QUANTICO State * VA Zip * 0022134

Service 10
- Select Service -

Organization * 11
- Select Organization -

Installation * 12
- Select Installation -

Office Symbol/Department * 13
- Select Command -

Cancel Save 14

Move to “Training Certificates” Tab

Sub-Steps:

- 1) Click “Training Certificates”

Welcome, STEVEN ELLINGTON. Help Desk: MCI COMFSB ServiceDesk@usmc.mil | (816) 915-3042 | Version: 2.1.1_14063 | Privacy Act

AutoSAAR My Profile SAARs Help Logout

My Profile:

Please complete your profile to continue. Missing Field(s): Email, Installation, Office Symbol / Department

Profile Information **Training Certificates**

* = required field.

Designation: * Military Civilian Contractor Citizenship: * US Foreign Other Receive Email Notifications: * Yes No Profile Datasources: DISS Marine Net MCTFS

Grade *
BWT 1-3

Display Name * Email Address * official govt. email only Phone Number * Job Title *

Supervisor or Authorized Approver Security Manager IA Training Coordinator

Supervisor / Authorized Approver is only required to create and submit a SAAR. It does not need to be entered to approve/deny SAAR(s). Security Manager is only required to create and submit a SAAR. It does not need to be entered to approve/deny SAAR(s). This field is optional. If a user is selected in it will override the default routing.

Supervisor not found

Official Mailing Address

Address Type Domestic Foreign

Address Line 1 * Address Line 2

City * State * Zip *

Service Organization * Installation * Office Symbol/Department *

Cancel Save

Upload Training Certificates

Sub-Steps:

- 1) Select the certificate your uploading
- 2) Select the file for the certificate
- 3) Please enter the date of completion of training
- 4) Return to the home page

Required Training

The following certificates are required for Marines:

- 1) **CYBERM00**
- 2) **HIPAA and Privacy Act Training**

The following certificates are required for Civilians:

- 1) **Cyber Awareness Challenge**
- 2) **Department of the Navy Annual Privacy Training**
- 3) **HIPAA and Privacy Act Training**

Welcome, STEVEN ELLINGTON, Help Desk: MCIComFSBServiceDesk@usmc.mil | (816) 915-3042 | Version: 2.1.1_14063 | Privacy Act

AutoSAAR 4 My Profile SAARs Help Logout

My Profile:

Profile Information | Training Certificates

Upload Certs

Document Type * 1 Cyber Awareness Challenge | Select File * 2 Choose a file Browse | Training Completion Date * 3 Upload

Current Certificates

Show 10 entries

Doc Type	File Name	Completion Date	File Size	Last Modified	Modified By	Delete
No data available in table						

Showing 0 to 0 of 0 entries Previous Next

Cyber Awareness Challenge

MarineNet Course = CYBERM0000 for military
MarineNet Course = CYBERC for civilian

<https://portal.marinenet.usmc.mil/content/mnet-portal/en/catalog.html?from=aem>

HIPAA and Privacy Act Training

JKO course = DHA US001

https://jkodirect.jten.mil/html/COI.xhtml?course_prefix=DHA&course_number=-US001

*****STOP ON THIS SLIDE*****

Notify Supervisor

- 1) Once you have updated your profile and added all required training certificates you need to notify your supervisor via email so that they can view and validate the training. This must be completed before you can move on to the next step.
- 2) If you added Mr. West as slide 3 stated above then email him at james.west@usmc.mil.
- 3) If you added your actual supervisor then they must log in to the Auto SAAR site and follow the first step above.

Welcome, STEVEN ELLINGTON. Help Desk: MCICOMFSBServiceDesk@usmc.mil | (816) 915-3042 | Version: 2.1.1_14063 | Privacy Act

AutoSAAR My Profile SAARs Help Logout

My SAARs:

Create SAAR

Show 50 entries Search:

View SAAR	System	Requestor	Requestor Installation	Created On	Status	Last Modified By
No data available in table						

Showing 0 to 0 of 0 entries Previous Next



*****Once your certs have been validated then you can proceed to create your SAAR for submissions.*****

Create SAAR

- 1) Click "Create SAAR"

Welcome, STEVEN ELLINGTON. Help Desk: MCICOMFSBServiceDesk@usmc.mil | (816) 915-3042 | Version: 2.1.1_14063 | Privacy Act

AutoSAAR My Profile SAARs Help Logout

My SAARs:

Create SAAR

Show 50 entries Search:

View SAAR	System	Requestor	Requestor Installation	Created On	Status	Last Modified By
No data available in table						

Showing 0 to 0 of 0 entries Previous Next



Create SAAR

Sub-Steps:

- 1) Scroll to bottom
- 2) Click "OMPF Viewer"
- 3) Scroll to top
- 4) Click "Submit"

Welcome, STEVEN ELLINGTON. Help Desk: MCICOMFSBServiceDesk@usmc.mil (816) 915-3042 | Version: 2.1.1_14063 | Privacy Act

AutoSAAR My Profile SAARs Help Logout

Create New SAAR:

Search Systems Filter by Organization

 MCICOM Portfolio System Manpower Information Portal (PDHRA)	 MCICOM Portfolio System Manpower Information Portal (START)	 MCICOM Portfolio System Manpower Information Portal (STR)	 MCICOM Portfolio System MARCENT Account Request - Server	 MCICOM Portfolio System Marine Corps Purchase Requirements System (MCPRS)
 MASTER DATA REPOSITORY Open Database Connectivity (MDR ODBC)	 MASTER SCHEDULING SUPPORT TOOL (MSST)	 MCICOM Portfolio System MCBOSS	 MCICOM Portfolio System MCEN	 MCICOM Portfolio System MCFMIS
 MCICOM Portfolio System MCTFS	 NEPA-PAMS	 OMPF Viewer	 SECRET TOTAL ALLOWANCE RECOMPUTATION TOOL (START)	 SPLUNK
 STRATIS-Enterprise NIPRNET	 TCPT-Enterprise NIPRNET	 TOTAL LIFE CYCLE MANAGEMENT - OPERATIONAL SUPPORT TOOL (TLCM-OST)		

Systems to Request:

- OMPF Viewer

Reset Selections Submit

Current Approved Roles

System	Installation	Roles
No data available in table		

Select Roles

Sub-Steps:

- 1) Check the “OMPF Viewer User” role
- 2) Enter justification for access (this will populate automatically once you place a check in the “OMPF Viewer User” box). **However, you must also include that you are a Security Manager employee/Marine and what unit you fall under.**
- 3) Click “Continue”

Welcome, STEVEN ELLINGTON.  Help Desk: MCICOMFSBServiceDesk@usmc.mil | (816) 915-3042 | Version: 2.1.1_14063 | [Privacy Act](#)

AutoSAAR [My Profile](#) [SAARs](#) [Help](#) [Logout](#)

Select Roles:

Please select at least one role and add justification for the following system:

OMPF Viewer

Type of Request:
 Initial Modification Deactivate

Available Roles:
 OMPF Viewer User

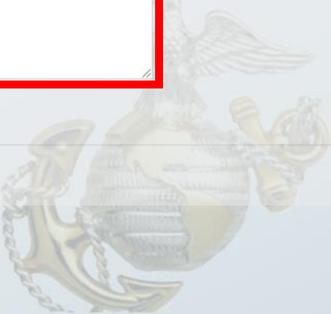
Justification for Access:

2

Justification must be less than 1,000 characters.

Request Authorized access Request Privileged access

[Continue](#) 3



Electronic Signature Confirmation

Sub-Steps:

- 1) Read acknowledgement
- 2) Click “Next”

Welcome, STEVEN ELLINGTON.  Help Desk:  MCIComFSBServiceDesk@usmc.mil |  (816) 915-3042 | Version: 2.1.1_14063 | [Privacy Act](#)

 AutoSAAR [My Profile](#) [SAARs](#) [Help](#) [Logout](#)

Electronic Signature Confirmation:

DD 2875 ADDENDUM 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 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 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 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

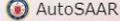


Electronic Signature Confirmation

Sub-Steps:

- 1) Read acknowledgement
- 2) Check “I have read..”
- 3) Click “E-Sign”

Welcome, STEVEN ELLINGTON.  Help Desk:  MCIComFSBServiceDesk@usmc.mil |  (816) 915-3042 | Version: 2.1.1_14063 | [Privacy Act](#)

 AutoSAAR [My Profile](#) [SAARs](#) [Help](#) [Logout](#)

Electronic Signature Confirmation:

By signing I agree to the following rules of behavior:

- I understand that I am providing both implied and expressed consent to allow authorized authorities, to include law enforcement personnel, access to my files and e-mails which reside or were created on Government IT resources.
- I will not conduct any personal use that could intentionally cause congestion, delay, or disruption of service to any Marine Corps system or equipment.
- I will not install or use any Instant Messaging client or peer-to-peer file sharing application, except that which has been installed and configured to perform an authorized and official function.
- I will not use Marine Corps IT systems as a staging ground or platform to gain unauthorized access to other systems.
- I will not create, copy, transmit, or retransmit chain letters or other unauthorized mass mailings, regardless of the subject matter.
- I will not use Government IT Resources for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but are not limited to: hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.
- I will not use Government IT resources for personal or commercial gain without commander approval. These activities include solicitation of business services or sale of personal property.
- I will not create, download, view, store, copy, or transmit materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited such as transmitting sexually explicit or sexually oriented materials.
- I will not use Marine Corps IT systems to engage in any outside fund-raising activity, endorse any product or service, participate in any lobbying activity, or engage in any prohibited partisan political activity.
- I will not post Marine Corps information to external news groups, bulletin boards or other public forums without proper authorization. This includes any use that could create the perception that the communication was made in one's official capacity as a Marine Corps member, unless appropriate approval has been obtained or uses at odds with the Marine Corps mission or positions.
- I will not use Marine Corps IT resources for the unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information, including computer software and data, that includes privacy information, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data.
- I will not modify or attempt to disable any anti-virus program running on a Marine Corps IT system without proper authority.
- I will not connect any personally owned computer or computing system to a DoD network without prior proper written approval.

 I have read and agree with the terms and conditions

 [E-Sign](#)

Questions

**Submit questions to Mr. James H. West for SAAR and
O-RMA permissions to:
James.west@usmc.mil**

