

# Access Request Management Service – ARMS

<https://odsf.mcw.usmc.mil/>



## ARMS

Access Request Management Service



Welcome to the Access Request Management Service (ARMS). ARMS allows you to request access to Marine Corps Financial Integrated Analysis System (MCFIAS).

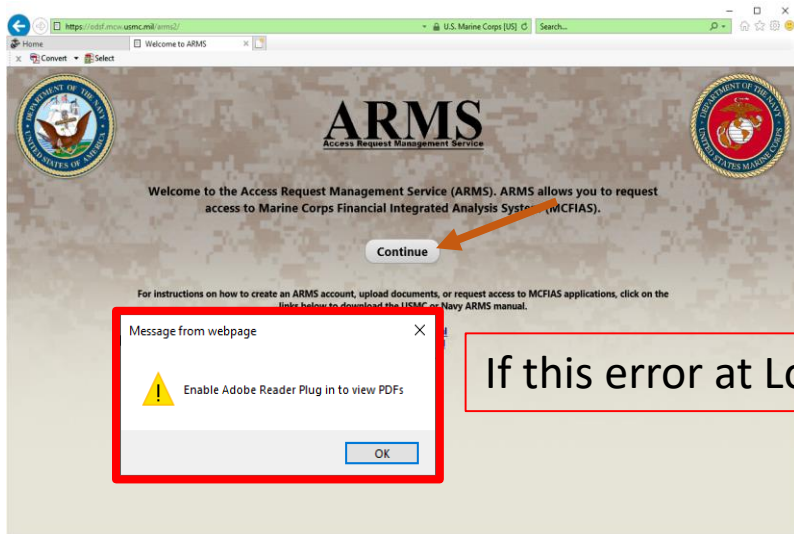
[Continue](#)

For instructions on how to create an ARMS account, upload documents, or request access to MCFIAS applications, click on the links below to download the USMC or Navy ARMS manual.

[USMC ARMS Manual](#)

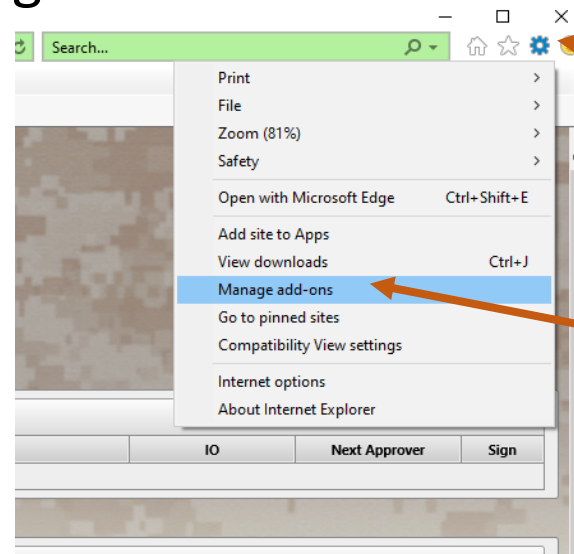
[Navy ARMS Manual](#)

# Enabling Adobe Reader Plug-In



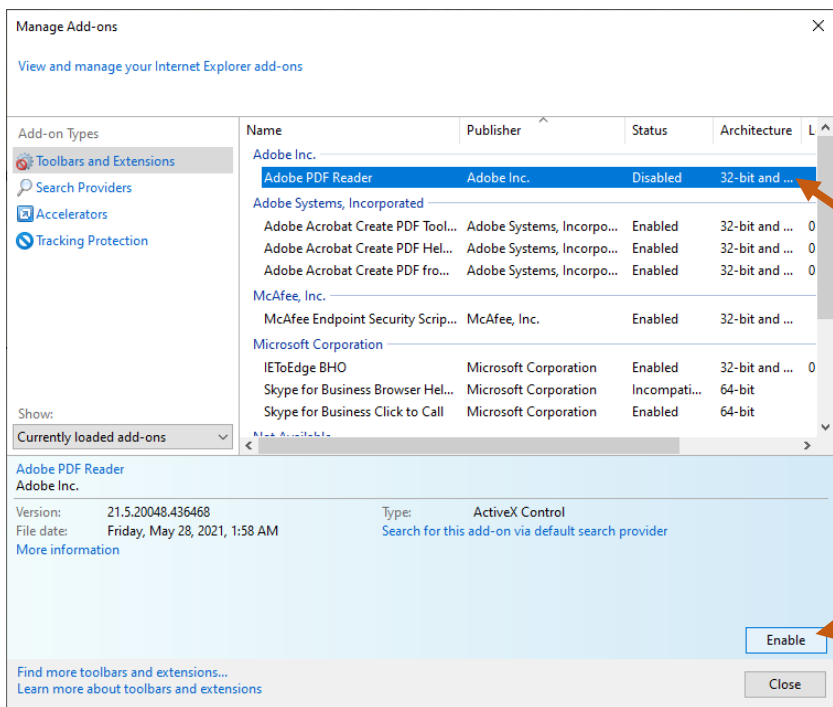
If this error at Login

ARMS requires the Internet Explorer browser



1. Go To Tools:

2. Manage add-ons



3. Select 'Adobe PDF Reader'

4. Enable

Some systems requiring enabling Adobe PDF Reader daily

| Title                         | View | Edit Date | Del Docu |
|-------------------------------|------|-----------|----------|
| DD-577 for Approving Official |      |           |          |
| Cyber Awareness Challenge     |      |           |          |

Adobe PDF Reader required for 'View' feature

# Internet Explorer Compatibility View Settings must be adjusted to complete ARMS requirements

## Compatibility View Settings



A screenshot of an Internet Explorer browser window. The address bar shows "ms2/" and "U.S. Marine Corps [US]". The page title is "Welcome to ARMS". The main content area features the "ARMS Access Request Management Service" logo and a "Continue" button. A context menu is open over the page, with "Compatibility View settings" highlighted. The menu options include Print, File, Zoom (86%), Safety, Open with Microsoft Edge (Ctrl+Shift+E), Add site to Apps, View downloads (Ctrl+J), Manage add-ons, Go to pinned sites, Compatibility View settings, Internet options, and About Internet Explorer.

## Compatibility View Settings (Continued)



A screenshot of the "Compatibility View Settings" dialog box. The title bar reads "Compatibility View Settings". The main heading is "Change Compatibility View Settings". There is a text input field for "Add this website:" with an "Add" button to its right. Below this is a list box titled "Websites you've added to Compatibility View:" containing "navy.mil" and "osd.mil", with a "Remove" button to its right. At the bottom, there are two unchecked checkboxes: "Display intranet sites in Compatibility View" and "Use Microsoft compatibility lists". A "Close" button is located at the bottom right. A link for "Internet Explorer privacy statement" is also present.

- Ensure that “USMC.MIL” is NOT in the first two boxes.
- Ensure that “Display intranet sites in Compatibility View” is NOT checked.
- Click “Close”, then fully CLOSE out Internet Explorer before attempting access again.



# Creating an ARMS Profile



**\*ONLY USE THE INTERNET EXPLORER (IE) BROWSER\***

1. Navigate to the MCFIAS landing page: <https://odsf.mcw.usmc.mil>

- Click on **“I have read this”**.
- From the landing page, select the following path: **ARMS -> USMC -> ARMS**.

2. When the ARMS screen displays, click the button that says **“Continue”**.



**Helpful Tips**  
Using a browser other than Internet Explorer will result in diminished ARMS functionality and an inability to submit access requests.

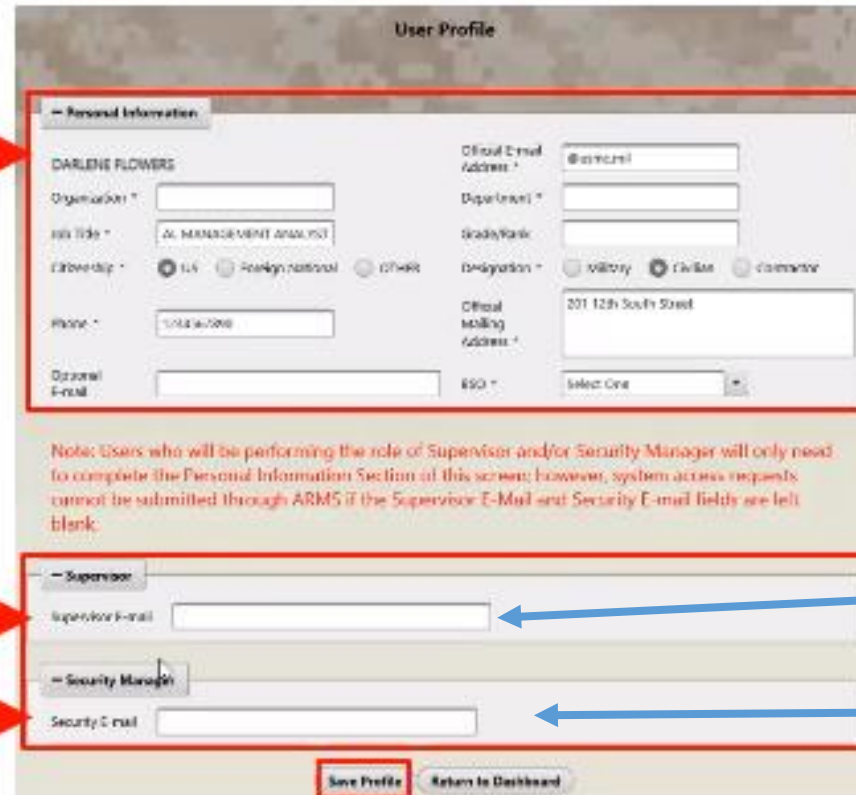
# Creating an ARMS Profile



3. Populate the following data fields to complete a User Profile:

- Official E-mail Address – **Government email**
- Organization – **Name of Budget Submitting Office (BSO)**
- Department – **Office Symbol/Department**
- Job Title
- Grade/Rank – **CTR, if Contractor**
- Citizenship – **US, Foreign National, or Other**
- Designation – **Military, Civilian, or Contractor**
- Phone Number (digits only)
- Office Mailing Address
- BSO – Select **BSO-27 USMC**
- Supervisor E-mail
- Security Manager E-mail

4. Click on **Save Profile** and the system will create your profile and direct you to the ARMS dashboard.



**Personal Information:**

DARLENE FLOWERS  
Organization \*  
Job Title \* AL MANAGEMENT ANALYST  
Citizenship \*  US  Foreign national  Other  
Phone \* 707440080  
Official Email Address \* @usmc.mil  
Department \*  
Grade/Rank \*  
Designation \*  Military  Civilian  Contractor  
Official Mailing Address \* 201 12th South Street  
BSO \* Select One

**Supervisor:**  
Supervisor E-mail

**Security Manager:**  
Security E-mail

**Note:** Users who will be performing the role of Supervisor and/or Security Manager will only need to complete the Personal Information Section of this screen; however, system access requests cannot be submitted through ARMS if the Supervisor E-Mail and Security E-mail fields are left blank.

**Save Profile** **Return to Dashboard**

Your Supervisor (listed in MyBiz+)

[townsend.milligan@usmc.mil](mailto:townsend.milligan@usmc.mil)

**Helpful Tip:** If the radio buttons or drop downs are disabled or not working properly, this is likely due to a browser Compatibility View setting. Please refer to slide 38 for instructions.

**Helpful Tip:** Users who only require the role of Supervisor and/or Security Manager are only required to submit the Personal Information section of this form. However, any user who also requires employee time user role must complete the remaining fields.

## Uploading Cyber Awareness Certificate



### 7. Attach the **Cyber Awareness Challenge Certificate**.

- For the Document Type, select “**Cyber Awareness Challenge**.”
- Enter the **Document Completion Date** (reference the “Date completed” field on your current Cyber Awareness Challenge Certificate).
- Then, click “**Upload**.” You will receive a successful upload confirmation message.

Please upload your documents

+ Browse Upload Cancel

Darlene Flowers Cyber Awareness Training Cert 2021 1120.pdf 18.2 KB

Document Type: Cyber Awareness Challenge

Document Completion Date: 11/20/2020

Close



### 8. Click “Close”.

Please upload your documents

+ Browse Upload Cancel

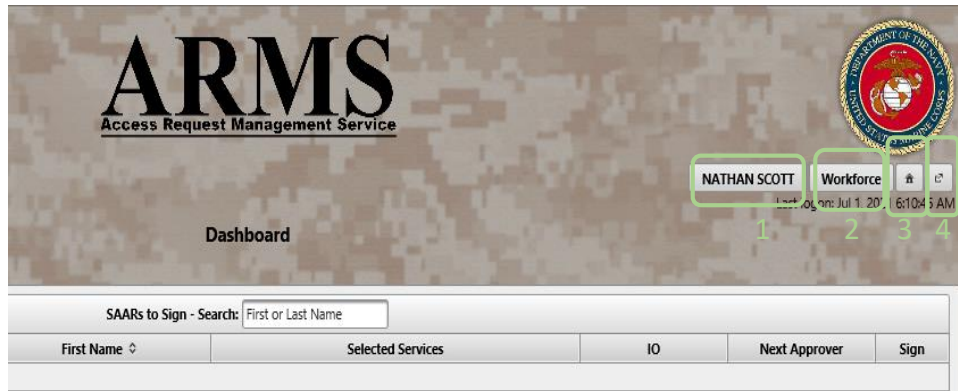
Document Type: Please Select

Document Completion Date:

Close

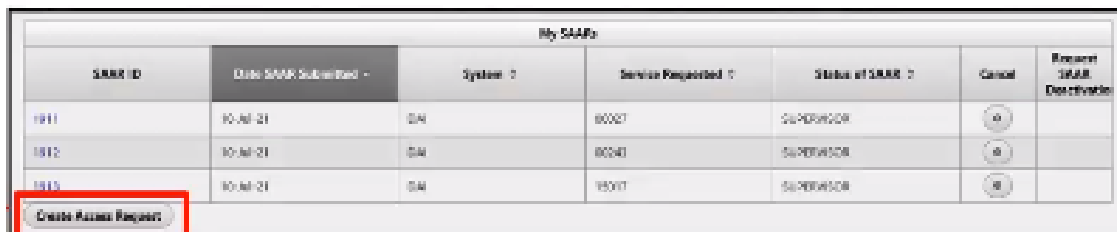


# ARMS Buttons Overview



1. User's Profile
2. Supervisors will have a Workforce button
3. Home is Dashboard
4. Logoff button

## Create Access Request In Dashboard





# ARMS

Access Request Management Service



Workforce

NATHAN SCOTT

Last login: Jul 16, 2021 5:57:47 AM

## Dashboard

SAARs to Sign - Search:

| SAAR ID        | Date Submitted | Last Name | First Name | Selected Services | IO | Next Approver | Sign |
|----------------|----------------|-----------|------------|-------------------|----|---------------|------|
| No SAARs found |                |           |            |                   |    |               |      |

| SAAR ID | Date SAAR Submitted | Status of SAAR                  | Cancel | Request SAAR Deactivation |
|---------|---------------------|---------------------------------|--------|---------------------------|
| 25012   | 24-Jun-21           | REJECTED (reason for rejection) |        |                           |

**Confirm Supervisor and Security E-mail Addresses**

Please confirm that your supervisor and security manager e-mail addresses are correct. If they are not, you can click the button below to update the e-mail addresses in your profile.

Supervisor E-mail Address: david.marzo@usmc.mil  
Security Manager E-mail Address: townsend.milligan@usmc.mil

**My Documents**

| Date Uploaded | Effective Date | Title                         | View | Edit Date | Delete Document | Date Val |
|---------------|----------------|-------------------------------|------|-----------|-----------------|----------|
| 06-24-21      | 06-24-21       | DD-577 for Approving Official |      |           |                 |          |
| 06-23-21      | 03-25-21       | Cyber Awareness Challenge     |      |           |                 |          |

# ARMS

Access Request Management Service

## Create Access Request

Please select one or more services:

| Service  | Description                                 |
|----------|---|
| ▶ ARMS   | ARMS Elevated Access Roles                  |
| ▶ DAI    | Defense Agencies Initiative                 |
| ▶ FDM    | Financial Data Management                   |
| ▶ MCFAD  | Marine Corps Funding Authorization Document |
| ▶ SMARTS | SABRS Management Analysis Retrieval Tools   |

UNCLASSIFIED//FOR OFFICIAL USE ONLY

For assistance with USMC ARMS requests, please contact the relevant information owner. To look up and co  
For assistance with Navy ARMS requests, please contact the Navy SIDI helpdesk at: [NAVY\\_SID](#)  
For assistance with MCFAD ARMS requests, please contact the MCFAD Helpdesk at: [PREXEC](#)  
For assistance with DAI ARMS requests, please contact the DAI Helpdesk at: [DAI\\_HelpDe](#)

[USMC ARMS Manual](#)  
[Navy ARMS Manual](#)

Access Request Management Service, version 2.0.50.2



Select: DAI > PROD > OTL (All Roles that Apply)

**All Civilian Employees**  
(SCROLL Down to CONTINUE)

**Civilian Supervisors select Both**

**Military Supervisors of Civilian Employees**

| Create Access Request                                       |                             |
|---|-----------------------------|
| Please select one or more services:                         |                             |
| Service ^   | Description                 |
| ▸ ARMS  | ARMS Elevated Access Roles  |
| ▾ DAI   | Defense Agencies Initiative |
| ▾ PROD  |                             |
| ▸ Full Financials   | Full Financials             |
| ▾ OTL   | Oracle Time and Labor       |
| ▸ 00027   | HQMC                        |
| ▸ 00146   | MCAS CHERRY POINT           |
| ▸ 00243   | MCRD SAN DIEGO              |
| ▸ 00260   | MCAF QUANTICO               |
| ▸ 00263   | MCRD PARRIS ISLAND          |
| ▾ 00264   | MCB QUANTICO                |
| <input type="checkbox"/> Limited Timekeeper                 | Limited Timekeeper          |
| <input checked="" type="checkbox"/> OTL Employee Time User  | OTL Employee Time User      |
| <input checked="" type="checkbox"/> OTL Supervisor Approver | OTL Supervisor Approver     |
| ▸ 00318   | MCB KANEOHE BAY             |
| ▸ 00681   | MCB CAMP PENDLETON          |
| ▸ 15017   | MCB CAMP MUJUK              |
| ▸ 20133   | II MEF                      |
| ▸ 20229   | MCB CAMP FUJI               |
| ▸ 20070   | MCB                         |

# DD Form 2875 SAAR Addendum Acknowledgements

HENDERSON HALL  
MCAFCC 29 PALMS

### SAAR Addendum

#### 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 provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

For assistance with MCFAD ARMS requests, please contact the MCFAD Helpdesk at: [PRFXCUTION@USMC.MIL](mailto:PRFXCUTION@USMC.MIL)  
For assistance with DD 2875 requests, please contact the DD Helpdesk at: [DD2875@NSA.MIL](mailto:DD2875@NSA.MIL)

HENDERSON HALL  
MCAFCC 29 PALMS

### Block 27 Acknowledgement

By signing block 11 I agree to the following rules of behavior:

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, 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 IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

HENDERSON HALL  
MCAFCC 29 PALMS

### Privacy Act

Authority: U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; and E.O. 9397 (SSN). Purpose: To collect personal and work-related information necessary to manage, supervise, and administer all aspects of DON programs for military, civilian, NAFI and contract members of the workforce.

Routine Uses: To assist command personnel on such matters as, but not limited to, preparing recall rosters and locators; maintaining accurate phone directories and manpower documents; contacting appropriate personnel in emergencies or during force mobilization; training the workforce; identifying routine and special work assignments; determining clearance for access control; assisting in manpower research studies; controlling the budget; travel expenditures, manpower and grades; maintaining statistics for employment; projection of retirement losses; labor costing; safety monitor reporting; tracking and reporting on the Navy's Information Assurance (IA) workforce; and similar administrative uses requiring personnel data. Any disclosures would be For Official Use Only as information is "close-hold" and shared with only those with an official "need-to-know". Some data, such as work location, communications and functional areas are generally available to the entire workforce. Access to remaining data is generally restricted to tiers of civilian and military supervisors ranging from immediate workplace supervisors to Site and Program Managers, Program Directors, and Military Commanders and their immediate staff. Administrative personnel will have access for purposes of maintaining the Intranet and TWMS databases.

Disclosure: Mandatory for Military. Mandatory for civilian, NAF, and contract personnel who have been designated by their organizations as "key", "emergency" or "critical" essential personnel. Mandatory for civilian, NAF, and contract personnel in positions that have been identified as part of the Navy's IA workforce in accordance with DOD 8570.01-M. Voluntary for all other civilian, NAF and contract personnel. In many instances, requested data (e.g., social security numbers and security clearances) may be available from other authorized databases. Failure by any workforce member to either provide or verify the accuracy of TWMS data may result in employees or their emergency POCs not being contacted in the event of recall, mobilization, emergencies, or other work or personal planning outcomes.

## Important Reminders



### DAI REMINDERS

- Users have the capability to check their ARMS account for an updated status of their DAI access request.
- If any request is rejected, the user **MUST** submit a **NEW** DAI request per the rejection feedback (vs. merely uploading a new Cyber Awareness Challenge Certificate or DD577).
- Users must maintain current Cyber Awareness Challenge Certificates to maintain their DAI access.
  - Any users with an expired certificate will be notified to renew their Cyber Awareness training and upload a valid certificate to maintain their DAI account.
  - DAI accounts may be suspended if the Cyber Awareness Challenge Certificate is expired.



## Best Practices

---



- To prevent invalid **Supervisor** or **Security Manager** issues, ensure that the supervisor and security manager have created a profile in ARMS.
- Ensure that the e-mail address for the Supervisor and Security Manager matches the e-mail address associated with their CAC.
- **Use Internet Explorer browser only.**
- Confirm that the proper level of access is being requested and the correct supporting documentation is provided.
- ARMS is currently just a repository for the electronic SAARs (and 577s). ARMS does not currently provision any access within DAI.
- Enable 'Adobe Reader' Plug-in to view PDFs.
- Check Compatibility Settings.