



Dear Valued DMDC Customer,

The Department of Defense (DoD) has mandated all applications to migrate to an approved DoD Enterprise Identity, Credential and Access Management (E-ICAM) solution for Identity, authentication, and provisioning approvals.

This document will provide awareness of what to expect after the transition to using Identity Provider (IdP) authentication. The following is an example scenario to provide an insight as to what you will see when logging into MRIS after IdP migration is complete.

### **IDP AUTHENTICATION**

1. Click the URL - [Military Recruiter Information Suite \(MRIS\)](#). The MRIS Splash page will appear.



## Military Recruiter Information Suite (MRIS)



The Military Recruiter Information Suite (MRIS) is a website that provides authorized users within the military recruitment community the ability to view reports, edit high school visitation records, and retrieve person and personnel data.

In accordance with the Department of Defense (DoD) Zero Trust Mandates, the MRIS application will be migrated to an approved DoD Enterprise Identity, Credential, and Access Management (E-ICAM) solution. For more information, please click on this link [MRIS E-ICAM IdP Authentication](#)

Access to this suite of applications requires the completion of a DD-2875. A copy of the form along with the instructions are provided below.

### Application Access Documents

[MRIS Access Form DD2875](#)

[MRIS Access Form DD2875 Instructions](#)

### Questions

DMDC Support Center (DSC): 800-477-8227

[Continue](#)

[Accessibility/Section 508](#) | MRIS is maintained by DMDC

The content in these files may contain CUI/PII information and should be handled IAW DoD, DHRA, and/or your organizations requirements. Per DoDI 5230.24: DISTRIBUTION STATEMENT C. Distribution authorized to U.S. Government agencies and their contractors for ADMINISTRATIVE OR OPERATIONAL USE (01Oct2021). Other requests for these documents shall be referred to DHRA/DMDC DSS Branch.

### *MRIS Splash Page*

2. Click the Continue button. The DMDC Consent and Acknowledgement Screen will appear.

Serving Those Who Serve Our Country




## Military Recruiter Information Suite (MRIS)

---

**Standard Mandatory DoD Notice and Consent**

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.

**Acknowledgement Of Responsibilities Of Receiving And Maintaining Privacy Act Data**

DATA YOU ARE ABOUT TO ACCESS COULD POTENTIALLY BE PROTECTED BY THE PRIVACY ACT OF 1974. You must:

- Have completed the necessary training with regards to Security Awareness and safe-guarding Personally Identifiable Information.
- Ensure that data is not posted, stored or available in any way for uncontrolled access on any media.
- Ensure that data is protected at all times as required by the Privacy Act of 1974 (5 USC 552a(1)(3)) as amended and other applicable DOD regulatory and statutory authority; data will not be shared with offshore contractors; data from the application, or any information derived from the application, shall not be published, disclosed, released, revealed, shown, sold, rented, leased or loaned to anyone outside of the performance of official duties without prior DMDC approval.
- Delete or destroy data from downloaded reports upon completion of the requirement for their use on individual projects.
- Ensure data will not be used for marketing purposes.
- Ensure distribution of data from a DMDC application is restricted to those with a need-to-know. In no case shall data be shared with persons or entities that do not provide documented proof of a need-to-know.
- Be aware that criminal penalties under section 1106(a) of the Social Security Act (42 USC 1306(a)), including possible imprisonment, may apply with respect to any disclosure of information in the application(s) that is inconsistent with the terms of application access. The user further acknowledges that criminal penalties under the Privacy Act (5 USC 552a(1)(3)) may apply if it is determined that the user has knowingly and willfully obtained access to the application(s) under false pretenses.

[Contact DMDC](#) | [Accessibility/Section 508](#) | [USA.gov](#) | [No Fear Act Notice](#)

OK

---

For **assistance** or to **report problems**, please call toll free: **800-538-9522** Commercial: **502-335-9980**.

### *Consent and Acknowledgement Screen*

3. Select OK to agree to proceed. The Registered User Logon Screen will appear.

Serving Those Who Serve Our Country




## Military Recruiter Information Suite (MRIS)

---

**Registered User Logon**

<b>AUTHORITY</b>	5 USC 301
<b>PURPOSE/ROUTINE USE</b>	Information you provide is used to verify your identity and usage of this website.
<b>DISCLOSURE</b>	Voluntary. However, if you fail to provide the requested information, DMDC will not be able to verify your identity. If your identity is not verified, you will be unable to gain access to the website.

Prevent illegal access of Privacy Act data by closing your browser before leaving your computer.

**Select Logon Method**

Smartcard (CAC, PIV)
 

Continue

[Logon Help](#)

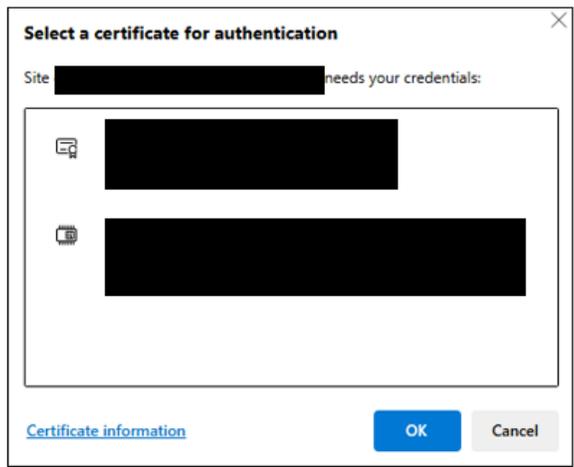
The material/information contained herein falls within the purview of the Privacy Act of 1974 and will be safeguarded in accordance with the applicable system of records notice and DLAR S40021.

---

For **assistance** or to **report problems**, please call toll free: **800-538-9522** Commercial: **502-335-9980**.

### *Registered User Logon Screen*

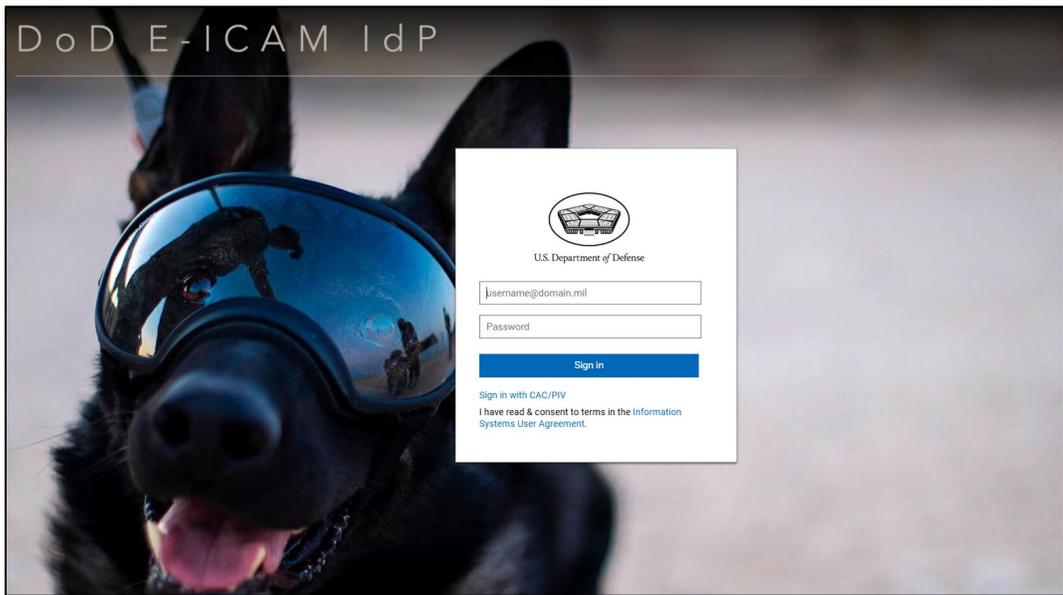
4. Select Smartcard (CAC, PIV) in the Select Logon Method, then click Continue. The certificate selection window will appear.



*Select a Certificate Screen*

5. Select your authentication certificate and then click OK. You will be redirected to the DISA IDP Authentication screen with a photo of a Dog wearing Goggles. This screen is known as 'The Doggle Screen.'

Note: If you have previously authenticated (i.e. logged into E-ICAM from a previous DoD application), the IDP authentication Doggle Screen will not appear, and you will be directly logged in by leveraging the E-ICAM Single Sign on (SSO) feature.



*DISA IDP Authentication 'Doggle' Logon Screen*

6. Select the linked text '[Sign In with CAC/PIV](#)' to proceed. Select the linked text to read the [Information Systems User Agreement](#) if needed; proceeding to login is consent to the

Agreement. Currently, CAC is required to login and authenticate.

7. The certificate selection window will appear again (step 4). Select your authentication certificate and then click OK.

8. You should now be logged into MRIS.

**Note:** Seeing 'The Doggle Screen' is expected during the application IdP authentication process.

Thank You for your continued dedication and collaboration!