# Table of Contents

Risk Management Information-Dive Jump Reporting System (RMI-DJRS) Getting Started ................. 2

1.1 Accessing RMI-DJRS ...................................................................................................................... 2

1.2 Requesting a New Account ........................................................................................................... 2

1.3 Risk Management Information (RMI) Homepage ......................................................................... 7

1.4 RMI Account Management ........................................................................................................... 8

1.5 Accessing Dive Jump Reporting System (DJRS) from RMI ........................................................... 9

1.6 DJRS Homepage .......................................................................................................................... 10

1.7 Resetting CAC Information ......................................................................................................... 10

1.8 Help Menu ................................................................................................................................... 11
Risk Management Information-Dive Jump Reporting System (RMI-DJRS) Getting Started

1.1 Accessing RMI-DJRS

RMI-DJRS is housed within the Air Force Safety Automated System (AFSAS). To access RMI-DJRS, users will need to navigate via the AFSAS URL: https://afsas.safety.af.mil

1.2 Requesting a New Account

**STEP 1:** Go to the RMI-DJRS website at https://afsas.safety.af.mil

**STEP 2:** Accept the US Department of Defense Warning Statement.

---

**US Department of Defense Warning Statement**

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.

**Agency Disclosure Notice**

The public reporting burden for this collection of information is estimated to average of 4 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Washington Headquarters Services, Executive Services Directorate, Information Management Division, 4800 Mark Center Drive, East Tower, Suite 02609, Alexandria, VA 22350-3100 [0701-TBD OMB Control Number]. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

**Accessibility/Section 508**

The U.S. Department of Defense is committed to making its electronic and information technologies accessible to individuals with disabilities in accordance with Section 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended in 1999. Send feedback or concerns related to the accessibility of this website to: the AFSAS Help Desk (COMM: 505-853-8200; DSN: 263-8200; AFSAS.AFSEC@us.af.mil) or DoDSection508@osd.mil. For more information about Section 508, please visit the DoD Section 508 website.

---

*Figure 1.2 Accepting DoD Warning Statement*
**STEP 3:** Create Basic Account form will automatically appear if you do not have an account.

Complete steps 4-9 as shown in Figure 1.2 Create an Account

---

**Figure 1.2.1 Create an Account**
STEP 10: Complete contact information

Figure 1.2.2 Predictive Text Example

Figure 1.2.3 Contact Information
Complete steps 11-14 as shown in Figure 1.2.4 Account Information

**STEP 11: Type of Account Requested-Basic vs. Elevated**
- In the “Account Information” block you will be asked what type of accounts you are requesting, either “Basic” or “Elevated”:
  - “Basic” Account is automatically granted and intended for most RMI-AFSAS users.
  - “Elevated” account is required for users to be granted access and roles in RMI-DJRS. “Elevated” accounts will require review and approval by your unit’s User Administrator.
  - For both “Basic” or “Elevated” accounts applicants must provide a detailed and meaningful justification addressing “why” they require access (i.e., what they will be using RMI-DJRS to do).
  - User Administrators will use this information to determine the appropriate permission levels needed (i.e., what can be done and for how long) for your account.
  - All DJRS roles are obtainable with an Elevated level account.

**STEP 12: Requested Roles**
- Both “DRJS: DJRS User” and “Workspace: US Navy/Marines” must be selected to gain access and roles in DJRS.

---

```
Step 11: Select “Elevated” Account Level

Step 12: Select “DRJS: DJRS User” and “Workspace: US Navy/Marines” for Requested Roles

Step 13: Type Justification “Required for DJRS Access” and include your Unit Manager’s name

Step 14: Click “Submit Application”
```

---

**Figure 1.2.4 Account Information**
STEP 13: Applicant’s Justification for AFSAS Access

- Specify requirement for RMI-DJRS access based on duties and responsibilities.
- This will be utilized to validate the requirement and grant access to DJRS.

STEP 15: Complete User Agreement

- Review the user agreement and Click “Continue.”
- Access to RMI-DJRS and the use of the data and reports withdrawn from it is predicated upon your acceptance of this user agreement. This user agreement covers:
  - Types of information contained in RMI
  - The restrictions on their reproduction and distribution
  - Notification and consent to monitoring
  - And concludes with a user agreement statement and concurrence
- You’ll receive an automated email after accepting the user agreement to associate your account with your CAC.
  - Check your email you used to register with.
  - Open the email and click the link provided or copy and paste the link into your browsers URL bar to associate your CAC.
1.3 Risk Management Information (RMI) Homepage

To access the RMI-DJRS Homepage:

Click on the “Home” link on the bottom left of the left-hand menu or click on the SIR Insignia. From the Homepage you can access the workflow and Menu.

The left-hand menu includes:

- Clicking over the choices offered will reveal more specific choices via sub menus.
- The left-hand menu is present depending on the display resolution (always present on large screen resolutions, minimized on smaller screen resolutions).
- To minimize or restore the left-hand menu, click on the “arrow” icon in the left side of the screen.
  - It contains frequently used choices that are always present and context sensitive choices whose appearance will come and go based upon what the user is working on and their assigned roles.

**NOTE:** Displayed Menu content will be determined by the security roles assigned to each user.

The RMI-DJRS Homepage lists:

- The RMI-DJRS Homepage lists all your workflow items awaiting review about halfway down the page. This should be a quick and easy way to see what your organization still has to complete. Below the “Work Items Awaiting Review” table, there is another table listing specifically your Late or Near Late Work Items to help each organization prioritize work to ensure no work items are late.
1.4 RMI Account Management

RMI-DJRS populates your name and assigned organization/office symbol combination from the information from your account profile and it is essential for the profile to be correct for many aspects of RMI-DJRS to work correctly.

- To review your account information and change it if necessary.
- Go to “ADMIN” ➔ ACCOUNT MANAGEMENT “My Account” on the left-hand menu bar.
- For information that you cannot change, select the “User Administrator” on the left-hand menu to identify your User Administrator who can correct this problem.
- User Administrators can search accounts under the Account Management menu on the left-hand menu bar.
- Go to “ADMIN” ➔ USER ADMINISTRATION “Homepage” ➔ ACCOUNT MANAGEMENT “Search Accounts”
1.5 Accessing Dive Jump Reporting System (DJRS) from RMI

**STEP 1:** Click “Dive and Jump Log” link on left-hand menu.
- Clicking the link will populate the “Dive and Jump Log” Sub-Menu.
  - This link is ONLY visible when DJRS Roles are granted.

**STEP 2:** Click “Homepage” link under the “Dive and Jump Log” Sub-Menu.
- This will populate the DJRS Homepage.

![DJRS Left Hand Menu](image)
1.6 DJRS Homepage

The DJRS Homepage displays quick links for easy access to Dive and Jump Data.
- Clicking on the quick links will display data for the option selected. For example, “Dive History” will display all the user’s approved dives.
- Users can filter data by clicking on the arrows located in the title column.
- Exporting and printing data is available by clicking the specified button once data is displayed.

![DJRS Homepage](image)

**Figure 1.6 DJRS Homepage**

1.7 Resetting CAC Information

When you get a new CAC card, RMI will send you to the RMI log-in page the next time you attempt to log in using your new CAC card.

**STEP 1:** Click on the “Re-link CAC with RMI Account” hyperlink. The system will navigate to the Re-link CAC with RMI Account page.

**STEP 2:** Enter your email address and click submit.

**STEP 3:** You will receive an email with a link to RMI. Your CAC will now be linked with your RMI account, and you will again be able to use your CAC and PIN to log into RMI.
1.8 Help Menu

- There are several informative documents on specific topics under “HELP” on the left-hand menu (go to “HELP”). Please explore the documents under this button for help on specialty topics within RMI and access to safety policy documents.

- **To find a copy of this guide**
  - Go to “HELP” → HELP “Help Files and User Guides.”

**Figure 1.8 Help Menu**

- **Getting Help** - Link will provide information about DJRS
- **Help Files and User Guides** - Link will navigate to the help documentation repository. User guides, help information, and videos will be posted in this location
- **AFSAS Policies** - Link will navigate to the list DOD, Air Force and Navy Policies