

## Instructions for Completing DD Form 2875

The Joint Medical Information Systems (JMIS) Office processes and creates all **Defense Health Program Systems Inventory Reporting Tool (DHP SIRT)** user accounts for all DHP funded managed systems. The procedures and data requirements to request and delete a DHP SIRT account are also provided below.

Please note that **ONLY** the August 2009 DD Form 2875 will be accepted when applying for a (DHP SIRT) user account. Earlier versions of the 2875, as well as the DISA Form 41, are obsolete and will not be accepted.

### *Notes on the DHP SIRT User Account Creation:*

- Original signatures or electronic CAC signatures may be used on all forms. In the interest of expediting processing, applicants and other signatories may scan the document containing the original signature creating a PDF and e-mail or fax the signed documents to the next person in the approval chain. When this method is used, each signatory must retain on file the copy of the document that contains their original signature, and provide it upon request.
- If the application is approved, the applicant and supervisor will be notified when your DHP SIRT account has been created.
- Part III of form 2875 must be completed by your Security manager. A valid security clearance and/or valid ADP/IT designation must be indicated.
- Completion of Annual Information Awareness Training must be the approved DoD IA Awareness Training.
- Will interim clearances be accepted? Yes, for ADP/IT-II/ADP/IT-I or SECRET/TOP SECRET. No for ADP-III/Confidential.

### *Notes on the DHP SIRT User Account Maintenance:*

Government DHP SIRT users and/or Government supervisors of contractor personnel must inform the DHP SIRT Program Office ([Lynne.Zetterholm.ctr@tma.osd.mil](mailto:Lynne.Zetterholm.ctr@tma.osd.mil)) when a DHP SIRT account is no longer required. A completed DD2875 requesting **deletion** of the account must be submitted when requesting to close a DHP SIRT account (see Pages 6-7).

*Forms should be hand-carried, mailed, emailed (encrypted), or faxed to the contact information provided below.*

### *Contact Information:*

Lynne Zetterholm

Tel. 703 681-8448 x.1221

Fax 703 681-7887 (include cover sheet, call or email first before faxing any documentation)

Email: [Lynne.Zetterholm.ctr@tma.osd.mil](mailto:Lynne.Zetterholm.ctr@tma.osd.mil)

Mailing Address: 5109 Leesburg Pike, Sky 6, Suite 900, Falls Church, VA 22041

**INSTRUCTIONS FOR COMPLETING DD FORM 2875  
INITIAL OR MODIFICATION**

○ <b>TYPE OF REQUEST:</b> Place an “X” in the INITIAL box if this is the first request for access, or place an “X” in the MODIFICATION box if you are resubmitting your form with corrections to your application.
○ <b>DATE:</b> Enter the Date in (YYYYMMDD) format. Example: 20090301.
○ <b>SYSTEM NAME:</b> Enter Defense Health Program Systems Inventory Reporting Tool (DHP SIRT).
○ <b>LOCATION:</b> Enter ATIC SKY 3, Suite 1600.
<b>PART I – The applicant completes the following user information when establishing or modifying their user account.</b>
○ Block 1: Enter your name (Last, First, Middle Initial).
○ Block 2: Enter your organization. Example: DHIMS, USN, TMA.
○ Block 3: Enter your office symbol/department.
○ Block 4: Enter your COMMERCIAL work phone number, including area code. Do not enter a DSN number.
○ Block 5: Enter your contact e-mail address.
○ Block 6: Enter your job title and grade/rank. Example: System Analyst, GS-14; COL, United States Army; or Contractor.
○ Block 7: Enter your official work mailing address.
○ Block 8: Indicate your citizenship status by placing an “X” in the US, FN (Foreign National), or OTHER box.
○ Block 9: Indicate your DOD affiliation by placing an “X” in the Military, Civilian, or Contractor box.
○ Block 10: IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS are <b>Mandatory</b> . ○ Check the box labeled “I have completed Annual Information Awareness Training.” ○ Enter the date when you last completed annual information assurance awareness training. Note: The training must be the DoD approved course and the date must be within one calendar year of your application date (YYYYMMDD format).
○ Block 11: Place your original signature or electronic CAC signature in this block.
○ Block 12: Enter the date of your signature in YYYYMMDD format. Example: 20090301.
<b>PART II – The applicant enters justification for access, type of access requested, and access expiration information. The Government Sponsor/Supervisor endorses the user’s justification for access, type of access required, and access expiration information. The Government Information Owner approves access to the system being requested. The JMIS Certificate Authority (CA) gives final approval of access to the system being requested.</b>
○ Block 13: Enter the reason a DHP SIRT account is required. Enter type of access required (see Attachment 1- DHP SIRT Roles).
○ Block 14: Place an “X” in the <i>AUTHORIZED</i> box.
○ Block 15: Place an “X” in the <i>UNCLASSIFIED</i> box.
○ Block 16: Place an “X” in the <i>“I certify that this user requires access as requested”</i> box.
○ Block 16a: If applicant is a <b>contractor</b> , please enter “See block 27” and use block 27 to enter the required information.
○ Block 17: Enter Government supervisor’s name.
○ Block 18: Government Supervisor must provide original signature or electronic CAC

signature.
○ Block 19: Enter the date of signature in YYYYMMDD format. Example: 20090301.
○ Block 20: Enter supervisor's organization or department.
○ Block 20a: Enter supervisor's GOVERNMENT email address.
○ Block 20b: Enter supervisor's COMMERCIAL work phone number, including area code. Do not enter a DSN number.
○ Block 21: Designated responsible person for accuracy and completeness of DHP SIRT data provides original signature or electronic CAC signature and enters name.
○ Block 21a: Enter COMMERCIAL work phone number, including area code for designated responsible person. Do not enter a DSN number.
○ Block 21b: Enter the date of signature in YYYYMMDD format. Example: 20090301.
○ <b>Block 22 - LEAVE BLANK</b> for JMIS Certificate Authority (CA) original signature or electronic CAC signature.
○ <b>Block 23 - LEAVE BLANK</b> for JMIS CA organization/department.
○ <b>Block 24 - LEAVE BLANK</b> for JMIS CA phone number.
○ <b>Block 25 - LEAVE BLANK</b> for JMIS CA signature date.
○ Block 26: Enter Applicant's name (Last, First, Middle Initial). Pre-populated with name entered in Block 1 if you use electronic form.
○ Block 27:
○ If applicant is a <b>contractor</b> , enter your company name, contract number, date current Period of Contract Performance ends, and CAC ID expiration date.
○ If applicant is <b>Military</b> , enter projected rotation date (YYYYMM).
○ If applicant is a <b>Government Civilian</b> , leave this block blank.
<b>PART III – The Security Manager completes the certification of background investigation or clearance information on the user requesting an account.</b>
○ Block 28: Enter the specific investigation performed for the applicant's clearance or ADP/IT designation. (NAC, NACI, NACL, ENTNAC, BI, SSBI, Pending/Other [list type]).
○ Block 28a: Enter the date the applicant's investigation was completed. In the case of an interim clearance, indicate the date the confirmation of the interim clearance was received.
○ Block 28b: Enter the applicant's security clearance or interim security clearance. (Confidential, Secret, Top Secret, Interim (list type)).
○ Block 28c: Enter the applicant's ADP/IT designation, if applicable. (I, II, III, Interim).
○ Block 29: Security manager's name.
○ Block 30: Security manager's COMMERCIAL work phone number, including area code.
○ Block 31: Security manager's original signature or electronic CAC signature.
○ Block 32: Security manager enters the date of signature in YYYYMMDD format. Example: 20090301.
<b>PART IV - LEAVE BLANK.</b> This section is completed by the JMIS when creating the account.

## Attachment 1 DHP SIRT Roles

Roles	Capabilities
General User	Users of DHP SIRT who can read any data on the DHP SIRT with the exception of budget data and shortly DBT/DBMSC Certification Data.
Organization Administrator	<p>A Service may elect to use or not use Organization Administrators as desired. Two organization administrators for each subordinate organization to the Military Service Medical Dept may be assigned, one as Primary and one as Secondary (for back-up purposes).</p> <p>A Component uses Organization Administrators to manage their assigned JMISO systems.</p> <p>Privileges include the following for any user belonging to the subordinate organization or any system for which the subordinate organization is the submitter.</p> <ul style="list-style-type: none"> <li>• Inactivate or delete DHP SIRT users (within the Organization)</li> <li>• Reactivate users whose accounts are expired or disabled (within Organization)</li> <li>• Add new systems belonging to the Organization with the minimum mandatory data elements(System Title, System Acronym, Type of System, and System Description)</li> <li>• Assign systems to a System Data Maintainer account for which the System Data Maintainer has authority to enter or update data (within the Organization)</li> <li>• Coordinate with the Service Administrator to have new users added, to change the role or status of a user account</li> </ul>
Service Administrator	<p>Services Administrators are responsible for managing the Service-managed systems. They are the main DHP SIRT POC for coordination of any DHP SIRT issues, along with maintaining Service user and Service system administrative data. There should be two service administrators for each Military Service Medical Dept, one Primary and one Secondary (for back-up purposes). Privileges include the following for any user record belonging to the Service or any system record for which the Service is the submitter. A Service may elect to use or not use Organization Administrators as desired.</p> <ul style="list-style-type: none"> <li>• Inactivate or delete DHP SIRT users (within the Service)</li> <li>• Reactivate users whose accounts are expired or disabled (within Service)</li> <li>• Add new systems belonging to the Service Medical Dept with the minimum mandatory data elements (System Title, System Acronym, Type of System, and System Description).</li> <li>• Assign systems to a System Data Maintainer account for which the System Data Maintainer has authority to enter or update data (within the Service)</li> <li>• Coordinate with the TMA DHP SIRT team to have new users added, to change the role or status of a user account</li> </ul>
System Data Maintainer	One or more per system at the discretion of the Service and the Organization. Maintains the record for a particular system(s) in DHP SIRT. Cannot add new systems to DHP SIRT, but once the record is established with minimum data elements, can add all the rest of the needed data. Can read/write data to any part of the DHP SIRT record for systems assigned to him/her with the exception of budget data.
Subject Matter Experts (SME)	SME is a person who is an expert in a particular functional area. SMEs check off a functional area as reviewed by clicking on the SME Review Completed field. The SME Reviewed Date and SME user name are set for that functional area. Any questions regarding particular fields in DHP SIRT can be directed to the assigned functional SME.
TMA Budget Manager	The TMA IT Budget Managers (Capital Asset Management & Oversight (CAM&O) are responsible for entering and validating the TMA budget submission to DoD. The TMA CAMO staff has the following privileges: VIEW all system records, and EDIT all funding data.
TMA IA Manager	TMA IA Managers are responsible for managing the information assurance status of all JMISO-managed systems. They are responsible for entering the IA data for all JMISO-managed systems. They can view all system records; add/change information assurance data for all systems. They may not delete records.

Roles	Capabilities
TMA DHP SIRT System Manager	The System Manager has the following privileges: View all parts of all records, edit parts of all records, delete records, add/delete/change user privileges and user groups.
Defense Business Certification (DBC) POC	DBC POC can update the Certification/Annual Review Record Approved by PCA for Upload to DITPR and view all records with the exception of budget data.
Records Manager	The Records Manager can update Records Management data and view all records with the exception of budget data.

**INSTRUCTIONS FOR COMPLETING DD FORM 2875  
DELETE AN ACCOUNT**

○ <b>TYPE OF REQUEST:</b> Place an “X” in the <b>DELETION</b> box if you are requesting deletion from the system.
○ <b>DATE:</b> Enter the Date in (YYYYMMDD) format. Example: 20090301.
○ <b>SYSTEM NAME:</b> Enter Defense Health Program Systems Inventory Reporting Tool (DHP SIRT).
○ <b>LOCATION:</b> Enter ATIC SKY 3, Suite 1600.
<b>PART I – Applicant enters full name.</b>
○ Block 1: Enter Applicant’s name (Last, First, Middle Initial)
○ Block 2: <b>LEAVE BLANK</b>
○ Block 3: <b>LEAVE BLANK</b>
○ Block 4: <b>LEAVE BLANK</b>
○ Block 5: <b>LEAVE BLANK.</b>
○ Block 6: <b>LEAVE BLANK</b>
○ Block 7: <b>LEAVE BLANK</b>
○ Block 8: <b>LEAVE BLANK</b>
○ Block 9: <b>LEAVE BLANK</b>
○ Block 10: <b>LEAVE BLANK.</b>
○ Block 11: <b>LEAVE BLANK</b>
○ Block 12: <b>LEAVE BLANK</b>
<b>PART II – Applicant enters reason for deletion of user account. Government Supervisor approves user account deletion.</b>
○ Block 13: Enter the reason for request to delete the account.
○ Block 14: <b>LEAVE BLANK</b>
○ Block 15: <b>LEAVE BLANK</b>
○ Block 16: <b>LEAVE BLANK</b>
○ Block 16a: <b>LEAVE BLANK</b>
○ Block 17: Enter Government supervisor’s name.
○ Block 18: Government Supervisor must provide original signature or electronic CAC signature.
○ Block 19: Enter the date of signature in YYYYMMDD format. Example: 20090301.
○ Block 20: Enter supervisor’s organization or department.
○ Block 20a: Enter supervisor’s email address.
○ Block 20b: Enter supervisor’s COMMERCIAL work phone number, including area code.
○ Block 21: <b>LEAVE BLANK</b>
○ Block 21a: <b>LEAVE BLANK</b>
○ Block 21b: <b>LEAVE BLANK</b>
○ Block 22: <b>LEAVE BLANK</b>
○ Block 23: <b>LEAVE BLANK</b>
○ Block 24: <b>LEAVE BLANK</b>
○ Block 25: <b>LEAVE BLANK</b>
○ Block 26: <b>LEAVE BLANK</b>
○ Block 27: <b>LEAVE BLANK</b>
<b>PART III – LEAVE BLANK</b>

○ Block 28: <b>LEAVE BLANK</b>
○ Block 28a: <b>LEAVE BLANK</b>
○ Block 28b: <b>LEAVE BLANK</b>
○ Block 28c: <b>LEAVE BLANK</b>
○ Block 29: <b>LEAVE BLANK</b>
○ Block 30: <b>LEAVE BLANK</b>
○ Block 31: <b>LEAVE BLANK</b>
○ Block 32: <b>LEAVE BLANK</b>
<b>PART IV - LEAVE BLANK.</b>