

# **RAPIDS**

## **Training Guide**

**A technical training reference**

---

**Revision 1.0**

**RAPIDS Version 6.2**

**RAPIDS Training Guide Revision Date**

**January 2003**

**Note: Please destroy any previous versions of this Training Guide.**

## Sections

<b>RAPIDS 6.2 Enhancements .....</b>	<b>xi</b>
<b>1 Overview .....</b>	<b>1-1</b>
<b>2 Infrastructure .....</b>	<b>2-1</b>
<b>3 DEERS/RAPIDS Roles .....</b>	<b>3-1</b>
<b>4 RAPIDS Help Resources .....</b>	<b>4-1</b>
<b>5 Becoming Familiar with RAPIDS .....</b>	<b>5-1</b>
<b>6 Using the RAPIDS Application.....</b>	<b>6-1</b>
<b>7 Training Scenarios .....</b>	<b>7-1</b>
<b>8 Using RAPIDS SVO Functions.....</b>	<b>8-1</b>
<b>9 Using RAPIDS SSM Functions.....</b>	<b>9-1</b>
<b>10 Deployable RAPIDS.....</b>	<b>10-1</b>
<b>Appendix A - Quick Reference Guide.....</b>	<b>A-1</b>
<b>Appendix B - Field Service Representatives Map.....</b>	<b>B-1</b>
<b>Appendix C – Joint Uniformed Services Personnel Advisory Committee .....</b>	<b>C-1</b>
<b>Appendix D – Joint Uniformed Services Medical Advisory Committee .....</b>	<b>D-1</b>
<b>Appendix E - RAPIDS Acronyms .....</b>	<b>E-1</b>
<b>Appendix F – Privacy Act Statement .....</b>	<b>F-1</b>

## Table of Contents

<b>RAPIDS 6.2 Enhancements</b> .....	<b>x</b>
<b>1 Overview</b> .....	<b>1-1</b>
1.1 Responsibilities of the DEERS/RAPIDS FSR.....	1-1
1.2 Objectives Of the RAPIDS Training Guide .....	1-1
1.3 Explaining DEERS and RAPIDS .....	1-2
1.3.1 DEERS/RAPIDS Features and Enhancements.....	1-2
1.3.2 Difference between DEERS and RAPIDS .....	1-3
1.3.3 What is a Rule-Based System? .....	1-3
1.3.4 Public Key Infrastructure.....	1-4
<b>2 Infrastructure</b> .....	<b>2-1</b>
2.1 RAPIDS Components .....	2-1
2.1.1 Common Access Card.....	2-1
2.1.2 Workstation.....	2-2
2.1.3 RAPIDS Server.....	2-3
2.1.4 DEERS Database .....	2-4
2.1.5 Issuance Portal .....	2-4
2.1.6 Certification/Certificate Authority.....	2-4
2.2 DISN/NIPRNet .....	2-5
2.3 Information stored in DEERS, RAPIDS Servers, and RAPIDS Workstations .....	2-5
2.3.1 DEERS Database .....	2-5
2.3.2 RAPIDS Servers .....	2-6
2.3.3 RAPIDS Workstations.....	2-6
2.4 RAPIDS Platform and Programming Languages .....	2-7
2.5 Secure Sockets Layer Architecture.....	2-7
2.6 Public Key Infrastructure.....	2-7
2.7 PKI, the CAC, and RAPIDS.....	2-8
<b>3 DEERS/RAPIDS Roles</b> .....	<b>3-1</b>
3.1 DEERS Site ID .....	3-1
3.2 DEERS Logon ID .....	3-1
3.3 Verifying Official.....	3-2
3.4 Super Verifying Official.....	3-3
3.5 Site Security Manager.....	3-3
3.6 Project Officer.....	3-4

3.7	Role of the RAPIDS Workstation.....	3-4
3.8	Responsibilities of the Card Recipient with Respect to PKI .....	3-5
3.9	Server and Remote Sites Responsibilities .....	3-5
3.9.1	Server Site Responsibilities .....	3-6
3.9.2	Remote Site Responsibilities .....	3-6
<b>4</b>	<b>RAPIDS Help Resources .....</b>	<b>4-1</b>
4.1	RAPIDS Web Resources .....	4-1
4.2	RAPIDS Online Help.....	4-2
4.3	RAPIDS Documentation.....	4-2
4.4	D/RAC, D/RSC-E, and DSO-A .....	4-2
4.4.1	When to Contact the D/RAC / D/RSC-E / DSO-A?.....	4-3
4.4.2	When to Contact My RAPIDS Server Site? .....	4-3
4.5	DEERS/RAPIDS FSRs.....	4-4
4.6	Project Officers .....	4-4
<b>5</b>	<b>Becoming Familiar with RAPIDS .....</b>	<b>5-1</b>
5.1	Activation of the Site and Site Security Managers.....	5-1
5.2	RAPIDS Passwords .....	5-3
5.3	Logging on to RAPIDS.....	5-4
5.3.1	First Time Login with Login ID and Password .....	5-5
5.3.2	Adding the Windows NT Login .....	5-5
5.3.3	Registering Certificates.....	5-8
5.4	Starting RAPIDS.....	5-9
5.5	Security (Locking the RAPIDS Workstation) .....	5-11
5.6	Opening a Family in RAPIDS .....	5-12
5.7	Taskbar and Taskbar Buttons .....	5-13
5.8	Notification Area .....	5-13
5.9	RAPIDS Menu .....	5-13
5.10	Quick Action Menu .....	5-14
5.11	RAPIDS Toolbar.....	5-15
5.12	RAPIDS Help (Using Online Help).....	5-16
5.12.1	RAPIDS Help from the Menu.....	5-16
5.12.2	Dialog Boxes and Dialog Tabs Help Button .....	5-17
5.12.3	RAPIDS Field Help .....	5-17
5.12.4	Online Help Command Buttons.....	5-18
5.12.5	Referring to RAPIDS Online Help .....	5-19
5.13	Family Tree.....	5-21

5.14	Family Tabs .....	5-22
5.14.1	Tasks Tab.....	5-22
5.14.2	Tree Details Tab.....	5-23
5.14.3	Sponsor Confirmation Tab.....	5-23
5.15	Person Window.....	5-24
<b>6</b>	<b>Using the RAPIDS Application.....</b>	<b>6-1</b>
6.1	Navigators.....	6-1
6.1.1	Open Family.....	6-1
6.1.2	Add Sponsor Navigator .....	6-2
6.1.3	Difference between a Personnel Category and a Personnel Condition .....	6-2
6.1.4	Add Dependent Navigator .....	6-4
6.1.5	Update Address Navigator.....	6-5
6.1.6	Suspend Benefits Navigator.....	6-6
6.1.7	Verify Dependents .....	6-7
6.1.8	DEERS/RAPIDS Fingerprint Capture Process.....	6-7
6.1.9	Bypass Fingerprint Capture Navigator .....	6-9
6.1.10	Create DD Form 1172 Navigator/DSO Scan Information.....	6-12
6.1.11	Create DD Form 1172-2 .....	6-14
6.2	RAPIDS Joint Data Model Smart Cards.....	6-15
6.3	Using RAPIDS to Issue the CAC .....	6-16
6.3.1	Create Card Navigator .....	6-16
6.3.2	CAC Issuance Process Flow .....	6-17
6.3.3	CAC Description.....	6-25
6.3.4	Certificate Revocation .....	6-27
6.3.5	Verifying CAC Certificates .....	6-28
6.3.6	Updating a CAC.....	6-30
6.3.7	Recycling a CAC .....	6-32
6.4	Troubleshooting for a CAC that Errors during Encoding.....	6-32
6.4.1	CAC Termination Procedures.....	6-35
6.5	PIN Maintenance .....	6-36
6.6	Online Processing .....	6-36
6.7	Offline Processing.....	6-37
6.7.1	Offline Modes for CAC Production.....	6-37
6.8	Smart Card Handling and Storage .....	6-39
6.9	CAC Consumables.....	6-40
6.9.1	Printer Ribbons, Laminate, and Toner Cartridges .....	6-40
6.9.2	Fargo ProL Printer Calibration Procedure .....	6-41

6.10	Alternate Identification Numbers .....	6-45
6.10.1	Temporary Identification Numbers.....	6-45
6.10.2	Foreign Identification Numbers.....	6-45
6.10.3	Civilian Identification Numbers .....	6-45
6.11	Using the Tools Menu.....	6-45
6.11.1	Site Information .....	6-46
6.11.2	DD Form 1172 Remarks List Updates.....	6-47
6.11.3	User Administration.....	6-47
6.11.4	Reports .....	6-47
6.11.5	Configuration .....	6-47
6.11.6	Printing the CAC Brochure.....	6-48
6.11.7	Customize .....	6-48
6.12	RAPIDS Site Locator.....	6-49
6.13	Printing Selected Views from RAPIDS.....	6-50
6.14	Screen Printing through RAPIDS and Windows .....	6-50
6.15	Shutting Down Your RAPIDS Workstation.....	6-51
<b>7</b>	<b>Training Scenarios.....</b>	<b>7-1</b>
7.1	Add a New Family to DEERS .....	7-1
7.2	Add Family Members .....	7-1
7.3	Update a Family Member Over 21 to Reflect Student Status.....	7-2
7.4	Update a Sponsor's Rank/Update Sponsor from Enlisted to Warrant Officer/Officer Rank with No Break in Service.....	7-2
7.5	Update a Military Sponsor's Marriage Status to Reflect a Joint Service Marriage.....	7-3
7.5.1	Update a JSM Sponsor to Become a Dependent Spouse Under the Other Sponsor's Record.....	7-3
7.5.2	Terminate a Dependent Under One Sponsor and Add Under Another .....	7-4
7.5.3	Transfer Children/Update entitlements between Sponsors in a JSM or Under Active Duty Sponsors .....	7-5
7.5.4	Terminate a Dependent Under One Sponsor and Add Under Another .....	7-6
7.6	Divorce a Sponsor from a Spouse Who Does Not Meet Unremarried Former Spouse Requirements .....	7-7
7.7	Divorce a Sponsor from a Spouse Who Meets URFS Requirements.....	7-7
7.8	Update a Child who is living with an Ex-Spouse .....	7-8
7.9	Retire an Active Duty Sponsor .....	7-8
7.10	Update Active Duty Sponsor to Temporary Disabled Retirement List (TDRL).....	7-9
7.11	Update TDRL Sponsor to Permanently Disabled Retired List (PDRL).....	7-9
7.12	Terminate Sponsor for End of Contract.....	7-10
7.12.1	Terminate Sponsor for End of Contract and Revoke CAC.....	7-10

7.12.2 Terminate ID Card/CAC without Terminating the Personnel Category or Relationship .....	7-10
7.13 Separate Sponsor from Active Duty and Add to Guard/Reserves .....	7-11
7.13.1 RCC definitions: .....	7-11
7.14 Separate Sponsor and Issue Transition Assistance (TA), Voluntary Separation Incentive (VSI), or Special Separation Benefit (SSB) and Guard/Reserve ID Cards .....	7-12
7.15 Issue ID Card for TA Sponsor or Family Member(s) After Medical Eligibility Has Expired 7-13	
7.16 Extend Guard/Reserve Contract End Date for Guard/Reserve Sponsor.....	7-13
7.17 Activate a Guard/Reserve Sponsor .....	7-13
7.18 Extend Active Duty End Date for a Guard/Reserve Sponsor .....	7-14
7.19 Deactivate a Guard/Reserve Sponsor .....	7-14
7.20 Separate Guard/Reserve Sponsor Involuntarily from the Selected Reserves .....	7-14
7.21 Update Inactive Ready Reserve (IRR) to Selected Reserves .....	7-15
7.22 Separate Guard/Reserve Sponsor from an Active Duty Mobilization.....	7-15
7.23 Transfer Guard/Reserve Sponsor from One Branch of Service to Another (e.g., Army Reserve to Air National Guard).....	7-15
7.24 Retire a Guard/Reserve Sponsor under the Age of 60 to Reflect Reserve Retired Category .....	7-16
7.25 Retire an Active Guard/Reserve Sponsor with Benefits and Pay Before Age 60 .	7-17
7.26 Change Reserve Retired Sponsor to Reflect Retired Category at Age 60 or Over	7-17
7.27 Add Court-Ordered Ward/Pre-Adopt to Sponsor .....	7-18
7.28 Change Relationship from Ward/Stepchild to Child When Sponsor Adopts the Ward/Stepchild .....	7-18
7.29 Medicare .....	7-19
7.29.1 Medicare Part A Reason Codes .....	7-19
7.29.2 Medicare Part B Reason Code .....	7-20
7.29.3 Add Medicare Benefits for a Family Member under Age 65 .....	7-21
7.29.4 Update Medicare Benefits for a Family Member Not Eligible for Medicare Part A After Age 65 .....	7-21
7.29.5 Update Medicare Benefits for a Family Member Not Eligible for Medicare Part A After Age 65, Purchasing Medicare Part B .....	7-22
7.29.6 Enter Medicare Part B for an aging in (turning age 65) beneficiary to reflect their TRICARE For Life Entitlement.....	7-22
7.30 Issue Non-commissioned NOAA Personnel ID cards .....	7-23
7.31 Graduate Service Academy to Active Duty .....	7-23
7.32 Deceased Sponsor .....	7-24
7.32.1 Create Deceased Sponsor (When the Sponsor is Not Showing on DEERS) and Add Unremarried Widow/Widower .....	7-24

7.32.2	Issue ID Card to Dependent of Deceased Reserve Retired Sponsor Who Died Before 60 <sup>th</sup> Birthday.....	7-25
7.33	Suspended Benefits.....	7-25
7.33.1	Suspend Benefits.....	7-25
7.33.2	Terminate Suspended Benefits .....	7-25
7.34	Reserve Officer Training Corps.....	7-26
7.34.1	Add a Reserve Officer Training Corps Sponsor.....	7-26
7.34.2	Terminate an ROTC Graduate Who is Awaiting Active Duty Assignment.....	7-26
7.34.3	Terminate a Reserve card for an ROTC Graduate Who Attains Active Duty Status the Day after Graduation.....	7-27
7.35	Terminate a Dependent Child that is Becoming a Sponsor .....	7-27
7.36	Add a DoD Civil Service Sponsor and Issue the CAC.....	7-28
7.37	Add a DoD Contractor.....	7-28
7.38	Add Civil Service/DoD Contractor Personnel Category to an Existing Sponsor..	7-29
7.39	Add a Benefit Eligible Condition to a Civil Service or DoD Contractor .....	7-30
7.40	Add Emergency Essential Civilian Sponsor and Issue Geneva Convention Card	7-30
7.41	Add Foreign Military Active Duty Member (NATO and Non-NATO) Serving in the United States Under Sponsorship of the DoD .....	7-31
7.42	Transitional Compensation for Abused Family Member .....	7-32
7.42.1	Update a Family Member Entitled to Transitional Compensation Due to Abuse (Sponsor on Active Duty Over 30 Days or Retirement Eligible).....	7-32
7.42.2	Divorce a Spouse Who is Eligible for Transitional Compensation from a Sponsor, Due to Family Abuse .....	7-33
7.43	Add Former Member .....	7-34
7.44	Create Temporary ID Card .....	7-34
7.45	Adding/Updating E-mail Certificates on an Existing CAC.....	7-35
7.46	Create DD Form 1172 and ID Card.....	7-35
7.46.1	DD Form 1172 .....	7-35
7.46.2	ID Card.....	7-36
7.46.3	Laminate the Teslin ID Card .....	7-36
<b>8</b>	<b>Using RAPIDS SVO Functions.....</b>	<b>8-1</b>
8.1	SVO Functions and Descriptions.....	8-1
8.2	Site Information .....	8-1
8.3	Remarks .....	8-1
8.4	RAPIDS Reports.....	8-2
8.4.1	How to Access Reports.....	8-2
8.4.2	Error Report .....	8-2
8.4.3	ID Card Report.....	8-3

8.4.4	Periodic Summary Report.....	8-7
8.4.5	Transaction Report.....	8-7
8.4.6	Exporting Reports.....	8-8
8.4.7	Deletion of Report Data.....	8-9
<b>9</b>	<b>Using RAPIDS SSM Functions.....</b>	<b>9-1</b>
9.1	SSM's Security Responsibilities.....	9-1
9.2	User Administration.....	9-1
9.2.1	Add New User with LRA Privileges.....	9-2
9.2.2	Activate User and Assign Roles.....	9-5
9.2.3	Update User Information (Update LRA Privileges, Update Name, Phone Number, Pay Grade, Title Roles).....	9-5
9.2.4	Terminate Users.....	9-7
9.2.5	View Site Roster.....	9-8
9.3	CAC stock and consumables.....	9-8
9.4	Policy and procedure compliance.....	9-8
9.5	Site Administration.....	9-9
9.6	Documentation and training.....	9-10
9.7	Inventory Logistics Portal.....	9-10
9.8	Using RAPIDS Configuration Utilities.....	9-10
<b>10</b>	<b>Deployable RAPIDS.....</b>	<b>10-1</b>
10.1	Overview.....	10-1
10.2	Before your unit deploys (Read now!).....	10-1
10.3	Establishing Communications for Deployable RAPIDS.....	10-2
10.3.1	Logging On to Deployable RAPIDS as Administrator.....	10-2
10.3.2	Adding a Machine Name.....	10-3
10.3.3	Configuration for Ethernet/Local Area Network Communications.....	10-4
10.3.4	Updating Ethernet/LAN Configuration.....	10-6
10.3.5	Configuration for Dial-up Communications.....	10-6
10.4	Deployable RAPIDS User Administration.....	10-9
10.4.1	Deployable RAPIDS and the SSM User Role.....	10-10
10.4.2	Generic User ID on Deployable RAPIDS.....	10-11
10.5	Logging on to Deployable RAPIDS.....	10-12
10.6	Creating ID Cards Using Deployable RAPIDS.....	10-12
10.7	Deployable Data Storage and Transmission.....	10-12
10.7.1	Uploading from Offline Repository to DEERS.....	10-13
10.7.2	Exporting Records to an Archive File.....	10-13

10.7.3 Importing an Archive File into Offline Storage..... 10-14

10.8 RAPIDS Theft Protection and the Key Master..... 10-14

10.8.1 Key Master password..... 10-15

10.8.2 Setting the Key Master password ..... 10-16

10.9 Deployable RAPIDS Limit to Offline and Audit trail Database Size ..... 10-16

**Appendix A - Quick Reference Guide.....A**

**Appendix B - Field Service Representatives Map..... B**

**Appendix C – Joint Uniformed Services Personnel Advisory Committee .....C**

**Appendix D – Joint Uniformed Services Medical Advisory Committee .....D**

**Appendix E - RAPIDS Acronyms ..... E**

**Appendix F – Privacy Act Statement..... F**

**Appendix G - Procedures for Moving RAPIDS Equipment..... G**

**Appendix H - Site ID Initial Request (DEERS) ..... H**

**Appendix I - QWS3270 Emulator ..... I**

**Appendix J – Special Character Reference .....J**

**Appendix K – Deployable Hardware Diagrams ..... K**

**Appendix L – Detailed Deployable Packing Instructions .....L**

## RAPIDS 6.2 Enhancements

The DEERS/RAPIDS development team constantly works towards improving and enhancing the RAPIDS application. Such enhancements are often invisible to the RAPIDS user community yet are vital to sustain the DEERS/RAPIDS system. This document identifies several of the most recent changes that affect the RAPIDS user community and the beneficiary population that they service. These enhancements include not only technological improvements, but also system changes driven by the RAPIDS user community input. Additionally many modifications have been implemented due to changes to policy and legislation affecting benefits.

When upgrading your workstation to version 6.2 (either by software push or CD) the updated RAPIDS Online Help file will be installed on your RAPIDS server. Each RAPIDS Site can choose when to download the Help file to their own RAPIDS workstations. This action must be completed at all RAPIDS workstations and can be completed by any RAPIDS VO: select **Help|Software Updates** from the RAPIDS menu. This download may take a few minutes based on your communications with the RAPIDS server.

### New Features

#### 1. Personnel Category and Condition Changes

- Allow RAPIDS Civilian users affiliated with the USCG, NOAA, and USPHS to be eligible for Common Access Card (CAC) issuance using the personnel category of “Other Federal Agency Employee”.
- Allow Retirees to also have a Guard or Reserve personnel category.
- Changed the process for activation of a Retiree so that the Retiree Personnel category must be terminated with the reason of “Activation”. At the end of the activation period, RAPIDS will create the Retirement personnel category with a new field, Personnel Original Retirement Date, to track the original date of retirement.
- Allow an Active Duty or Reserve sponsor to become an Academy Sponsor based on Separation Program Designator (SPD) code.
- Allow the termination of On Active Duty condition with a Special Operation code and separation from the Reserves on the same day.
- Display citizenship status for all personnel categories in the Characteristics view.
- Change the minimum sponsor age from 16 to 15.
- Allow for enlisted sponsors to be separated without a Re-enlistment (RE) code if they are being separated within 90 days of enlistment.
- Require the VO to terminate the current Agency/Sub agency before allowing the sponsor to join another Agency/Sub agency.
- Modified the Civilian personnel condition not to extend beyond the personnel category end

date.

- Modified to display “Prisoner” instead of “Military Prisoner”.
- Modified the personnel category element, “Other Government Agency Employee” to “Other Federal Agency Employee”, except for Presidential Appointee for DoD affiliates.

## 2. Relationship and Relationship Condition Changes

- Request confirmation of a Divorce decree when entering an Un-remarried Former Spouse (URFS) 20/20/20.
- Require that the VO verify dependents when adding a new personnel category to an existing sponsor.
- Display the “Date of Marriage” in the Former Spouse Qualification Screen.
- Modified relationship condition of “sponsor provides 50% support” to “sponsor provides over 50% support”.
- Updated the next verification date on Former Spouses to match card expiration date.
- Corrected the benefits for Military Sealift Command dependents accompanying their Sponsor overseas.

## 3. Fingerprint

- Automatically sense and verify the presence of VO fingerprint during the logon process.
- Issue a CAC for individuals with hard-to-capture fingerprints or no fingers using **the Bypass Fingerprint Match/Verification** screen and the SSM’s digital signature.

## 4. Medicare

- Capture the Health Insurance Claim Number (HICN) when entering or modifying Medicare.
- Retrieve default Medicare benefits at age 65.
- Allow addition/termination of Medicare B up to 90 days in the future.

## 5. CACs and Teslin ID Cards

- Allow the issuance of CACs on workstations configured as Deployable.
- If a problem occurs during CAC issuance, or if a card is terminated within one day of issuance for reason of “Damage/Failure”, the VO is shown a dialog with the return code that needs to be written on the surface of the CAC before it is returned.
- Replacement of the progress bar during encoding with the display of progress using the Encoding Summary dialog. The dialog now shows the current step with an animated icon, checking off steps that succeed, and shows status messages at the top. The average encoding time, the time elapsed for the current card encoding, and the time elapsed for the current encoding step appear on the dialog.
- For Federal Agency employee CACs, display the Great Seal, "Federal" component, and

"Civilian" status.

- Allow the middle name to be printed on Teslin cards.
- Replace the “Non-NCO” rank with “PVT/LCPL” rank on Marine Corps CACs.
- Instruct the VO to enter the first 20 characters of the chip ID on the “Chip ID Capture” Dialog.
- When terminating expired cards, the VO is given the default termination reason of “expired”.
- Moved the message prompting VO to remove card recipient’s CAC from reader until after transactions are saved to DEERS or saved offline.
- Modified RAPIDS so Date of birth is legible even if member wears a dark uniform.
- Removed the ability to print pre- Optical Variable Device (OVD) CAC surface.

## **6. Person Identifiers**

- No longer create DEERS Dependent Suffix (DDS) based barcodes for dependents when TIN or FIN is present.
- When the option to update a Dependent TIN/SSN is disabled, RAPIDS will provide the reason. For example, when a dependent is also a sponsor.
- Mandate FIN to begin with a ‘9’ in Offline mode.
- Display the ID type before the TIN/FIN on the ID Card.

## **7. Reports**

- Display fingerprint override and fingerprint bypass in the RAPIDS Transaction Audit Trail Report.
- Display PIN Change and Email Updates on RAPIDS Transaction Report.
- Display the status of each certificate in ID Card Report.

## **8. Other Enhancements**

- Capture and display Organ Donor Information
- Print updated DD Form 1172 (July 2002)
- Print updated DD Form 1172-2 (October 2002)
- Automatically turn on Num Lock when RAPIDS is started.
- Display Certificate Revocation Status Code on Certificate screen.
- Display the Chip ID on ID Card view.
- Allow future RAPIDS releases to support a wider range of cameras using TWAIN interface.

## **Modified Features**

- Modified Begin and End dates for abuse scenarios to match DD Form 2698.
- Terminate Direct Care benefits if family members' SSN is not provided after a grace period.
- Removed Dental Premium Screens from Other Contracts Plans.
- Identify Civilian Health as secondary payer.
- The Verify Dependents dialog box no longer displays Terminated dependents.
- Require an Estimated Date of Retirement for civilians.
- Print updated CAC publicity brochure.
- Updated DD Form 1172 so Direct Care benefits do not display if not entitled.
- Updated DD Form 1172 to print "INDEF" end date for Permanently Disabled Retired List.
- Set system time on RAPIDS workstations based on the date and time returned from DEERS transactions.

## 1 Overview

The Defense Enrollment Eligibility Reporting System (DEERS) was developed by the Department of Defense (DoD) in response to a congressional mandate to improve the control and distribution of available military health care services. DEERS provides computerized information service for the enrollment of individuals eligible for Uniformed Services benefits. To reduce potential fraud, waste, and abuse associated with obtaining benefits available to members of the Uniformed Services and their family members, the Real-time Automated Personnel Identification System (RAPIDS) was established in 1981 and implemented a more secure method for producing identification (ID) cards. The DEERS database and RAPIDS application are integrally linked because RAPIDS is one of the primary means for updating information in DEERS. The DEERS Division of the Defense Manpower Data Center (DMDC) maintains the DEERS database. The DEERS/RAPIDS Operations Division (D/R Ops Div) of the DMDC is responsible for the RAPIDS program.

RAPIDS software allows its users to create, modify, and use personnel information stored in DEERS to provide ID cards and related personnel support to persons who are eligible for Uniformed Services benefits or ID cards. RAPIDS transactions account for more than 90 percent of the online transactions that keep the DEERS database current.

On 10 November 1999, the Deputy Secretary of Defense signed a memorandum that mandated the creation of a DoD CAC. At that time, it was decided that the ID card for Active Duty, Guard/Reserve, and certain Civilian populations would be redesigned to allow for the issuance of the CAC through the RAPIDS software.

---

### 1.1 Responsibilities of the DEERS/RAPIDS FSR

DEERS/RAPIDS FSRs are assigned regionally and support the diverse needs of the user population by providing information, onsite training, telephone and online support, problem resolution, and a vehicle for users to communicate their program requirements. A complete listing of the FSRs, with addresses and telephone numbers, can be found in *Appendix B* of this training guide.

---

### 1.2 Objectives Of the RAPIDS Training Guide

The main objectives of the RAPIDS Training Guide are to provide users with:

1. Serve as a learning tool to provide a basic knowledge of the DEERS database, the DoD Public Key Infrastructure (PKI), and the role of RAPIDS within the infrastructure.
2. Support day to day operations as an illustrated technical, procedural and informational reference for RAPIDS users.

3. Provide each RAPIDS site with an illustrated technical resource for continued training of existing personnel and training of new personnel as assigned to the RAPIDS site.
4. Provide instructions for using the RAPIDS application, printing DD Forms 1172 and 1172-2 and issuing the automated ID card (including CAC), without assistance.
5. Provide examples and instructions for implementing smart card and Public Key Infrastructure technologies to issue the CAC and authenticate users for the DoD PKI.

---

### 1.3 Explaining DEERS and RAPIDS

RAPIDS is designed to automate the following functions.

1. Update the DEERS database. RAPIDS workstations communicate with the DEERS database, allowing the user to update sponsor and family information in the DEERS database quickly and easily.
2. Determine eligibility for benefits. RAPIDS can analyze a beneficiary's data to determine the correct benefits and eligibility period, based on the DoD Eligibility Tables.
3. Create DD Forms 1172, the Application for the Uniformed Services Identification Card and DEERS Enrollment and DD Form 1172-2, Application for Department of Defense Common Access Card, DEERS Enrollment. RAPIDS generates and prints the DD Form 1172 and 1172-2 upon the user's command.
4. Produce ID cards. RAPIDS can turn the data entered by the user and the benefits and entitlements derived by the system into the Uniformed Services ID card, Geneva Conventions ID card, or DoD Civilian ID cards.
5. Implement the use of smart card and PKI technologies to issue the CAC and authenticate users for the PKI.

With the 10 November 1999 mandate from the Deputy Secretary of Defense to create a DoD CAC, RAPIDS version 6 was developed to include the hardware, software, communications, and security requirements to issue the CAC.

#### 1.3.1 DEERS/RAPIDS Features and Enhancements

One of the greatest advantages of the DEERS architecture is that DoD entitled benefits are accurately tracked and determined. The entitlement verification process is simplified by determining eligibility and benefits derived by the system, which eliminates the need to memorize or research codes to complete screens. Data is entered into fields for sponsors and family members through screens that consist of questions, lists, and options. It is designed to operate in a Windows-based environment and incorporates multiple system enhancements.

The Windows-based environment provides the following timesaving, user-friendly features.

1. Extensive online and context sensitive Help with step-by-step instruction.

2. Graphical user interface to include icons, pull-down menus, buttons, trees, and lists. These make the RAPIDS application easier for the user.
3. Task Navigators assist users through various types of transactions.
4. The DD Form 1172/1172-2 and ID cards are displayed on screen as they appear on paper.
5. Customizable workspace.

The system enhancements ensure the following features.

1. Compliance with DoD policy and regulations.
2. Consistent benefit determination.
3. Quick adaptation to legislative changes.
4. Consistent rule set.
5. Storage of personnel history.
6. Storage of more complete Medicare information.
7. Storage of more medical benefits information.

### **1.3.2 Difference between DEERS and RAPIDS**

DEERS is the database that tracks personnel and medical DoD benefits. The DoD operates one of the largest health care systems in the world. DEERS has rules that determine benefits based on the beneficiary's data and status in DEERS. Tracking and determining personnel and medical DoD benefits help reduce the fraud and abuse of DoD benefits. Also, it ensures that all beneficiaries receive the benefits to which they are entitled.

RAPIDS is the application software that allows users to communicate with the DEERS database. RAPIDS determines benefits and using the same rules as DEERS, allows users to issue machine-readable automated ID cards, including the CACs, and print the DD Form 1172 and DD Form 1172-2. Additionally, it provides a means to update sponsor and family member information in the DEERS database.

The DEERS and RAPIDS data is protected under the Privacy Act Statement (10 U.S. Code 133; Executive Order 9397, November 22, 1943, (Social Security Number); and Title 5, United States Code Section 301). RAPIDS users can only confirm information on the sponsor or family member. As required by the Privacy Act of 1974, the operator cannot volunteer personal information from the DEERS record.

### **1.3.3 What is a Rule-Based System?**

RAPIDS is a rule-based system, which means that it determines the correct benefits and entitlements for each beneficiary based upon the information that is provided to it by DEERS

and the RAPIDS user. Routinely, RAPIDS users are relieved of the time consuming responsibility of looking up entitlements in eligibility tables each time a beneficiary requires service. In addition, software updates incorporate changes in legislation and eligibility rules.

RAPIDS is capable of determining the benefits for which a sponsor or family member is eligible by following a series of conditions or rules. This eliminates the need for the user to monitor legislative changes and eligibility rules. The capability has been added to enter, store, and track multiple associations between the individual and various DoD organizations.

### **1.3.4 Public Key Infrastructure**

The Internet is widely used throughout the Federal Government and the DoD. The Federal Government portion of the Internet is referred to as the National Information Infrastructure (NII), and the DoD portion is referred to as the Defense Information Infrastructure (DII). The NII and the DII are vital to conducting the day-to-day business of the Government. The DII has become critical to the command and control of combat operations.

Users of the NII and DII must be confident that an adequate level of security exists to protect the information stored, transmitted, and processed on them. One mechanism that supports information system security is public key technology. Public key technology is a form of cryptography that uses separate electronic keys for digitally signing, encrypting, and decrypting information. In order for public key technology to be trusted, it requires a supporting infrastructure, the PKI. The DoD PKI is being created to manage NII and DII users' identities and public keys. More information about the DoD PKI and CAC can be found in *Section 2.7* of this training guide.

## 2 Infrastructure

Physically RAPIDS consists of servers and workstations located throughout the continental United States (CONUS), Alaska, Hawaii, United States Virgin Islands, Cuba, Puerto Rico, the Middle East, throughout Europe, and throughout the Western Pacific Theater. As previously mentioned, RAPIDS workstations and servers communicate with the DEERS database using the DII.

---

### 2.1 RAPIDS Components

RAPIDS extends beyond the application loaded on a site's workstation. An extensive database and communications infrastructure has been developed to support the functionality of RAPIDS. With the inclusion of the PKI requirements, this infrastructure has been enhanced with changes to existing and addition of other components. The elements of this enhanced infrastructure are detailed in the RAPIDS Security SOP and include each of the following components:

1. CAC enabled with Local Registration Authority (LRA) privileges
2. RAPIDS workstation
3. RAPIDS server
4. DEERS database
5. Issuance Portals
6. DoD Certificate Authority

The server elements are connected using the Defense Information Systems Network (DISN) / Nonclassified but Sensitive Internet Protocol Router Network (NIPRNet).

#### 2.1.1 Common Access Card

The CAC is issued to eligible Active Duty military personnel including the Selected Reserves, DoD civilian employees, and eligible contractor personnel.

The CAC is made of plastic (polyvinylchloride [PVC]) and contains an integrated circuit chip (ICC) with 32 kilobytes (KB) of memory storage. The standard (code 39) and two-dimensional (PDF417) bar codes contain demographic and card management information. Unlike the permanence of bar codes, the data stored on the chip can be updated or erased. The magnetic stripe has the ability to store building access or financial information. The ICC contains identification, demographic, card management, benefits, digital certificates, the cardholder's private keys and other application specific data. The digital certificates can be used to verify or authenticate the cardholder via a computer system or network, encrypt information, and sign digital documents, such as electronic mail.

The Java card used for CAC contains a Java Application Programming Interface (API), a simplified subset of the Java programming language. Cryptographic features allow for encryption and decryption. Three main applications (applets) are resident on the CAC after it is issued from a RAPIDS workstation: (1) PIN Management, (2) PKI Certificate and Keys Management, and (3) Demographics Data Management.

A PIN is used for cardholder identity verification and security. Services provided by the PIN Management applet include: verification of the PIN, changing the PIN, unlocking the card, managing the number of unsuccessful PIN attempts (four) before locking the chip, and managing minimum (six) and maximum (eight) PIN lengths.

The PKI applet manages signature encryption and decryption, key generation, and certificates, but it does not contain the certificates. At the time of issuance, the card recipient's CAC can be populated with three certificates: Identity certificate, E-mail Digital Signature certificate, and E-mail Encryption Certificate. Identity and E-mail Digital Signature private keys never leave the card. The E-mail Encryption private keys are generated off the card and escrowed by the Certification Authority (CA). It is important for both the CAC recipient and the VO to understand the importance of updating RAPIDS with the correct work e-mail address. The correct work e-mail address is used to derive the e-mail certificate. If the address on the certificate does not match the address actually being used, the application may reject the certificate.

The Demographics Data application is used to perform individual identification, identify eligibility to medical and non-medical DoD-provided benefits, perform card tracking and maintenance, and aid in manifesting. Demographics data is separated into the following four distinct groupings.

1. The Person applet is used for individual identification.
2. The Personnel applet is used to identify an individual's affiliation to the DoD.
3. The DoD Benefits applet is used to identify an individual's eligibility to DoD-provided benefits.
4. The Other Benefits applet provides maintenance of the meal entitlement code.

### **2.1.2 Workstation**

The workstation component is the hardware and software that actually produces the physical ID card, the CAC, and the DD Form 1172 or 1172-2. Workstations include a personal computer (PC), digital camera, laminator, bar code scanner, fingerprint scanner, laser printer, surge suppressor, and a communications device connecting the workstation to the RAPIDS server. Workstations configured to issue the CACs will also have a plastic smart card printer, PIN pad, USB port device, and two smart card readers/encoders. Refer to the RAPIDS Hardware Guide for a detailed technical specification of the RAPIDS workstation.

A workstation may connect to the RAPIDS server via a modem, a local area network (LAN)/wide area network (WAN) connection, or a simple cable. For auditing purposes, RAPIDS

workstations must have access to a RAPIDS server to generate an ID card and print a DD Form 1172 or 1172-2. The workstation is not responsible for the creation of PKI certificates. RAPIDS workstations require connection to the Issuance Portal and Certificate Authority to produce the CAC. **Precautions:** If the Fargo ProL Printer must be moved, be sure to recalibrate the printer when finished. Fargo ProL printers may not be switched between RAPIDS workstations by the site. The pan/tilt mechanism of the digital camera is very delicate and is not designed for manual operation. For large camera movements, use the handle on the camera stand; for smaller camera movements, use the keyboard/mouse with the RAPIDS application. Moving the camera manually results in broken or stripped gears.

When returning any RAPIDS hardware for maintenance be sure to remove items that are not part of that hardware prior to packing and shipping. Please take special precautions for the FARGO Pro-L printer to remove all of the Common Access Card cardstock, printer ribbons (which contain Privacy Act information) and laminate. Check to ensure there is no jammed cardstock in the printer. On the Laser Jet paper printers, remove the toner cartridge and paper. Remove any CD-ROMs or diskettes from the RAPIDS Workstation.

**Important Note:** RAPIDS users must be aware that the RAPIDS workstations or servers should not have commercial or private software installed on the hard drives for organizational or personal use. Examples of unauthorized software are screen savers, MS Word, MS Excel, e-mail or Internet Service provider (ISP) software, etc.

### 2.1.3 RAPIDS Server

The RAPIDS server consists of a personal computer, Uninterruptible Power Supply (UPS), an Ethernet switch, a multi-port connector box, optional modems (as required), a surge suppressor, and, in some instances, a laser printer. The RAPIDS server will also receive a smart card reader/encoder to allow the RAPIDS Site Security Manager (SSM) to log on to the server directly for performing administrative duties, such as user administration.

The RAPIDS transaction database is the name for the Oracle server that resides on a RAPIDS server or a RAPIDS deployable or stand-alone system. The RAPIDS transaction database is responsible for storing site information (i.e., activated users, 1172 remarks) and audit logs for every DEERS transaction. The transaction database is located on a RAPIDS server for all workstations that are connected to it, so that user accounts can be managed and reports can be generated centrally. However, remote workstation users can generate the reports and perform user administration on the RAPIDS server for their site from their local RAPIDS workstation. The transaction database is located on the local workstation for deployable and stand-alone systems.

RAPIDS servers may provide communications services for directly connected and remotely located workstations, which are used to access the DEERS database. The workstations are connected to a server system via modems, direct connections, a LAN, or a WAN. The RAPIDS server should remain powered on at all times. The server should not be powered off unless so mandated by the DEERS/RAPIDS Assistance Center (D/RAC) / DEERS/RAPIDS Support Center – Europe (D/RSC-E) / DMDC Support Office – Asia/Pacific (DSO-A).

On Deployable RAPIDS laptops, the server and workstation software are combined.

#### 2.1.4 DEERS Database

DEERS is an Oracle relational database that resides on a Sun server located in the Auburn Hills Service Management Center (AHSMC), Auburn Hills, Michigan. DEERS is the database that tracks personnel and medical DoD benefits. A knowledge base of rules makes the determination, based on data entered by the user. Every individual eligible for Uniformed Services benefits should have personal information stored in DEERS.

#### 2.1.5 Issuance Portal

The RAPIDS workstation uses a central trusted system called the Issuance Portal for cryptographic operations. The RAPIDS workstation always uses the Issuance Portal to communicate with the CA. The Issuance Portal “talks” to the CAC and writes all of the commands to the ICC.

The Issuance Portal is responsible for generation of the card recipient’s e-mail encryption keys and for updating the card recipient’s CAC with the encryption private key and all three certificates (one identity and two e-mail). The card recipient’s CAC generates the signature keys for identity and e-mail certificates and provides the public keys back to the Issuance Portal. The Issuance Portal interacts with the CA on behalf of the RAPIDS VO. The crypto module is never present at the RAPIDS workstation and accessible only when an authorized RAPIDS VO has signed onto the workstation, authenticated himself/herself to DEERS with their PKI certificate and a biometric (fingerprint) verification. Only after those verification and validations occur, can the Issuance Portal, with the cryptomodule capability, be accessed.

All CACs must have an identity certificate at a minimum. When an e-mail address is provided, the E-mail Encryption and E-mail Digital Signature certificates are also generated and stored on the CAC.

#### 2.1.6 Certification/Certificate Authority

The DoD CAs are systems that issue and manage digital PKI certificates for DoD end users. A certificate is a computer-generated record that ties a user’s identification with the user’s public key in a trusted bond. This trust is based on a registration process that is automated by the CA. The Secure Sockets Layer (SSL) session encrypts all communications between the CAC, Issuance Portal, and CA. Public and private keys help ensure that the information transmitted between computers is secure.

DMDC’s Issuance Portal interacts with DISA’s CA on behalf of the RAPIDS VO. DMDC controls the intermediate step. The Issuance Portal funnels all requests from RAPIDS to the CA. The entire process of working with the Issuance Portal requires the RAPIDS operator to be recognized as a VO by DEERS and a Local Registration Authority by DISA’s CA.

Three types of servers support the DoD PKI.

1. DoD Root CA servers authorize subordinate CA servers to issue certificates to users in the DoD PKI. The DoD Root CA is the common point of trust for all certificates issued by the DoD PKI.
2. The subordinate CAs generate, sign, and issue the certificates, escrow encryption e-mail certificates, manage Certification Revocation Lists (CRL), and post certificate information and CRLs to the Directory Server.
3. Directories are secured and trusted repositories of information, usually collected during the registration process. The Directory Server stores the certificates containing public keys for all registered individuals/entities and makes these available to other individuals/entities that need to verify a certificate or use a public key for encryption. The directory server stores the CRL.

---

## 2.2 DISN/NIPRNet

In September 1991, the Office of the Secretary of Defense (OSD) directed the Defense Information Systems Agency (DISA) to implement the DISN. The DISN is the DoD's consolidated worldwide enterprise level telecommunications infrastructure, which provides the end-to-end information transfer network for supporting military operations.

The DISN scope is defined in terms of the network geographical coverage, type of telecommunications services provided, and underlying initiatives to support those services. The DISN infrastructure encompasses CONUS, Alaska, Hawaii, United States Virgin Islands, Cuba, and Puerto Rico-sustaining segment; segments in Europe and the Western Pacific theaters; a space segment; and a deployable capability. Specific to RAPIDS users, the DISN provides the data transport path between the RAPIDS servers and the DEERS database. The DISN also provides the transport path between the RAPIDS workstations and servers connected via WANs. The NIPRNet, SIPRNet, and DISA Asynchronous Transfer Mode (ATM) Network are DoD internetworks that provide unclassified and classified computer networking service for official DoD business.

---

## 2.3 Information stored in DEERS, RAPIDS Servers, and RAPIDS Workstations

### 2.3.1 DEERS Database

The DEERS database is located at the AHSMC, Auburn Hills, Michigan, and stores the following types of information.

1. Person (sponsor/dependent) data in an Oracle database. (The term "dependent" is used in this software application to refer to a family member whose eligibility for entitlements is dependent upon his/her relationship to a sponsor).
2. Security information for all DEERS users.

3. Master look-up tables where any updates are made and then replicated down to the RAPIDS server and workstations (these tables contain valid information for the various fields, e.g., eye color table containing all possible DEERS eye colors).

### **2.3.2 RAPIDS Servers**

RAPIDS servers store the following types of information.

1. The RAPIDS application.
2. Site-centric information, such as user information for all sites/users assigned to a server.
3. Auditing data for the RAPIDS workstations connected to the server.
4. Report data (the result or end product of the audits for the RAPIDS workstations connected to the server).
5. Offline records (before transmitting to DEERS for the RAPIDS workstations connected to the server).
6. Lookup tables (If a change to a table is made on DEERS, the new information is sent to the RAPIDS servers. These tables are then replicated from the servers to the RAPIDS workstations).
7. Site specific remarks for the DD Form 1172 for RAPIDS workstations attached to the server.

### **2.3.3 RAPIDS Workstations**

RAPIDS workstations store the following elements.

1. The RAPIDS application.
2. Microsoft (MS) Access database containing tables (e.g., eye color/hair color).
3. PKI Certificate Registration information (ActivCard Gold).

To accommodate the production of the CAC and to meet the DoD PKI requirements, the RAPIDS workstations include the following new hardware peripherals.

- Two smart card readers/encoders - one for the VO's identity certificate for logging on and one to read/encode the card recipient's ICC during CAC issuance.
- PVC card printer - to print the CAC.
- Personal Identification Number (PIN) pad - for the CAC recipient to enter their PIN.
- Universal Serial Bus (USB) port device – to provide additional ports to connect the CAC-production peripherals to the RAPIDS workstation.

## 2.4 RAPIDS Platform and Programming Languages

RAPIDS servers and workstations use the Windows NT operating system. The RAPIDS application is written in C++ using object-oriented analysis and design techniques. It uses an Oracle database on the server and an MS Access database on the workstation. The DEERS modules use COBOL, Customer Information Control System (CICS), Aion DS knowledge base programming (artificial intelligence), C coding, and an Oracle database that resides on a Sun server at the AHSMC. The Java card used for CAC contains a Java API, a simplified subset of the Java programming language.

---

## 2.5 Secure Sockets Layer Architecture

Under the CAC configuration, RAPIDS establishes an SSL session using the VO's PKI identity certificate and key pair. SSL is a protocol that allows for the secure transfer of sensitive information over the Internet. SSL technology takes a message and runs it through a set of steps that scrambles or encrypts the message. This is performed so that the message cannot be read while it is being transferred. When the intended recipient receives the message, SSL unscrambles the message, verifies that it came from the correct sender (authentication), and then verifies there has been no tampering with the message. The VO's certificate is checked against the CA's CRLs. With the use of SSL in RAPIDS version 6, RAPIDS achieves Federal Information Processing Standard Level 2 Compliance. The RAPIDS workstation communicates with the DEERS database via Federal Information Protection Standards (FIPS) 140-1 compliant Secure Sockets Layer (SSL) encryption. Communications between the RAPIDS workstation, the Issuance Portal and the Certificate Authority are secured using SSL.

The RAPIDS application data is encrypted using a symmetric key established during the SSL session construction. The Netscape Security Services Library and the VO's identity certificate establish an SSL session with the DEERS SSL server and the Issuance Portal.

Some users of RAPIDS version 6 may notice that additional time is required to issue the CAC in comparison to issuing the teslin cards. The increased level of security in communications and the additional coordination between systems well justify this additional processing time.

---

## 2.6 Public Key Infrastructure

PKI is not a thing, but a capability enabled by the application of specific protocols, services, and standards that support public key cryptography. The DoD PKI is a system of CAs, Registration Authorities (RAs), directories, client applications, and servers that model trust and allows for secure/encrypted electronic data transfers/transactions. A PKI is essential in supporting Public Law 103-355, the Federal Acquisition Streamlining Act of 1994, which requires the broad use of Electronic Commerce and Electronic Data Interchange (EDI) by Federal agencies. In his 1997 Management Reform Memorandum number 16, Deputy Secretary of Defense, Dr. John Hamre, directed the development of a DoD-wide PKI that supports information security. PKI provides the framework and services for the generation, production, distribution, control, and accounting of certificates. Certificates contain the user's unique digital identity and public key. PKI is used to answer the following two questions:

- Who are you?
- Can I trust that you are who you say you are?

Public key technology is often referred to as asymmetric or a two-key system. Each user has a pair of keys; the keys are not the same but match up in a unique way. One key is kept only by the user and is called the private key. The other key is widely distributed and is called the public key. These electronic key pairs provide users with two important capabilities. The first is the ability to digitally sign a document. The second is the ability to encrypt and decrypt messages. When digitally signing a document, the sender's private key is used to sign it, and the recipient uses their public key to verify the signature. When sending an encrypted message, the sender uses the recipient's public key to encrypt the message, and the recipient's private key is used to decrypt the message.

A certificate is a computer generated digital record that ties a user's/entity's identity with their public key in a trusted bond. This trust is based on the individual's/entity's identity being verified then registered by the RA, and the certificates being created, signed, and issued by a trusted server known as a CA. As long as a certificate is signed by the trusted CA and the trusted CA's signature can be verified. Any tampering with the certificate can be readily detected.

Public and private keys help ensure that the information transmitted between computers is secure. Simply having the keys alone is of no benefit; to make use of them, the user must have a PKI enabled application that provides the following advantages.

1. **Confidentiality or privacy:** protecting data from anyone who is not authorized to view it.
2. **Data Integrity:** protecting data from unauthorized modification during transmission, storage, and processing.
3. **Identification:** verifying the identity of the person.
4. **Authentication:** verifies identity through something the person possesses, something they alone know, or some part of them (fingerprint).
5. **Non-repudiation:** because of the authentication, PKI prevents the e-mail sender from denying he or she sent the message. This is also the case when any document is signed with the individual's digital signature certificate. This is known as non-repudiation.

It is imperative that each individual secures their CAC and does not share or write down the PIN protecting it.

---

## 2.7 PKI, the CAC, and RAPIDS

DoD named RAPIDS as the system to produce the new DoD ID card, CAC, which utilizes this smart card and PKI technology. RAPIDS had the existing hardware and card management infrastructure to complete this task, thus ensuring full and consistent use of existing capabilities. The DoD Local Registration Authority (LRA) role is encompassed within the RAPIDS VO, Super Verifying Official (SVO), and/or SSM role. RAPIDS is used to verify an individual's

identity, collect information that is to be entered into public key certificates, and to forward requests for certificates to the CA. In addition, the CAC was designated as the primary token carrier for the DoD-wide PKI.

The DoD CAC employs smart card and PKI technology. Each CAC contains a unique ICC that has read and write capabilities and is capable of containing a significant amount of data, as well as a PIN selected by the cardholder. This PIN acts as a security code for the cardholder, preventing others from using the card to fraudulently obtain access to benefits, such as commissary and exchange privileges.

The CAC is the size of a credit card and contains the ICC that is used to store a moderate amount of data, a magnetic stripe, a Code 39 bar code, and a two-dimensional PDF417 bar code. The CAC also contains a color photograph and printed text. As DoD implements applications that use these automated technologies on the CAC, data can be added, modified, or removed from the card as needed. These cards are used for visual identification, access to buildings and controlled spaces, and access to DoD computer networks and systems. Eventually, users will be able to use their CACs to send and receive secure e-mail messages and access secure Web sites. Component specific uses may also be added.

Through RAPIDS, up to three PKI certificates and their associated private keys are stored on the CAC: identity, e-mail encryption, and e-mail digital signature. Certificates contain user identity data, the validity period for the certificate, digital signature, and the private key portion of the public/private key pair used in public key encryption. Managing keys and certificates through a PKI helps an organization establish and maintain a trustworthy network environment. Information encrypted by a public key can only be decrypted with a private key (and vice versa).

RAPIDS is the first DoD PKI enabled application to be implemented worldwide. The VO is required to insert his/her CAC into a smart card reader/encoder attached to the RAPIDS workstation to log on. At this point, RAPIDS uses the ActivCard Gold utility to manage communication between the CAC and Windows. The VO's DEERS ID is accessed from the CAC and the VO then enters his/her six to eight digit PIN to initiate the log on. Under the CAC configuration, RAPIDS begins to establish an SSL session using the VO's PKI identity certificate and key pair. To complete the log on process to DEERS, RAPIDS prompts the VO to place his/her finger on the RAPIDS fingerprint scanner. The fingerprint is then verified against the fingerprint information stored on DEERS. Once verified, the log on process is complete. The VO's CAC must remain inserted at all times while using the RAPIDS workstation.

With a few exceptions, all the members of these target populations are issued a CAC.

- Active Duty members.
- Selected Reserve and National Guard members - This includes members in these categories who are on Active Duty. There may be some exceptional situations in which members in other Reserve categories will receive a CAC, because they require an electronic card to gain physical access to controlled areas or logical access to Government computers.

- Civilian DoD employees, including Non-appropriated Fund (NAF) and foreign national employees - Card issuance to foreign military will follow the same rules as those for foreign national DoD employees.
- Certain Other Federal Agency employees, including Civilians working for the Public Health Service, the Coast Guard, and the National Oceanic and Atmospheric Administration.
- Designated DoD contractors who require an electronic card to gain physical access to controlled areas or logical access to Government computers. Contractor CACs will display a green stripe on the front of the card.
- Presidential Appointees.

Contractor CACs will display a visible green stripe along the front of the card while non-US citizen CACs will display a red stripe. In the event that a non-US citizen contractor is issued a CAC, the red stripe will be printed.

The following populations continue to be issued teslin Uniformed Services identification and privilege cards, unless a CAC is issued for exceptional conditions

- Reserve members who are in the Standby Reserve, Individual Ready Reserve, or the Inactive National Guard, i.e., components that are not classified as Selected Reserve. These members will receive a DD Form 2 (Reserve).
- Designated DoD contractors who do not require an electronic card to gain physical access to controlled areas or logical access to government computers, but do require an ID card to conduct government business or a privilege card to access authorized DoD benefits. This mostly applies to contractors who are employed overseas or are considered emergency essential because they are likely to be assigned overseas, are serving overseas, or are employed at US installations where benefits are authorized locally. These individuals will receive DD Forms 2750 or 2764, as applicable.

The following other populations will receive the teslin Uniformed Services identification and privilege cards, as indicated, without exception.

- Reservists not receiving a CAC receive a DD Form 2 (Reserve).
- Retirees with full retirement benefits receive a DD Form 2 (Retired).
- Reserve retirees receive a DD Form 2 (Reserve Retired) until they reach age 60, at which time they qualify for full retirement benefits and the DD Form 2 (Retired).
- Family members of Active Duty, Reserve, and retired (with full retirement benefits) sponsors will receive DD Forms 1173 and 1173-1. While there are some exceptions, children below the age of ten do not receive any cards.

Local conditions and authorities may dictate exceptions to the basic guidelines. Target populations and card applicability are summarized in the table below. In almost all cases, CACs will be issued with an ICC. Card entries in **bold** indicate those cards that will be in circulation after the target date for completion of migration to the CAC. Cards that expect to be phased out by that date are shown in *light italics*. Cards shown in normal type can be expected to have some

subgroups that will not receive CACs and will continue to receive teslin cards.

<b>Member Category (Personnel Category Code)</b>	<b>CAC (ICC/Non-ICC)</b>	<b>Teslin Card (Form)</b>
Active (A)	ICC	2ACT
Academy student - does not include Officer Candidate School (J)	ICC	2ACT
Reserve (Selected) - mobilized or on Active Duty for 31 days or more (V)	ICC	2ACT
Reserve (Standby/IRR) - mobilized or on Active Duty for 31 days or more (V)	ICC	2ACT
Reserve (Selected) - not on Active Duty or on Active Duty for 30 days or less (V)	ICC	2RES
Reserve (Standby/IRR) - not on Active Duty or on Active Duty for 30 days or less (V)	N/A	<b>2RES</b>
National Guard (Selected) - mobilized or on Active Duty for 31 days or more (G)	ICC	2ACT
National Guard (ING) - mobilized or on Active Duty for 31 days or more (G)	ICC	2ACT
National Guard (Selected) - not on Active Duty or on Active Duty for 30 days or less (G)	ICC	2RES
National Guard (ING) - not on Active Duty or on Active Duty for 30 days or less (G)	N/A	<b>2RES</b>
Presidential Appointee (B)	ICC	2750/2764
DoD civil service – requiring electronic access, are emergency essential, or are serving overseas (C)	ICC	2765/2764/2750
Lighthouse service (L)	N/A	<b>2765</b>
American Red Cross (M)	N/A	<b>2765</b>
Other Federal Agency (non-DoD) - Civil Service (O)	ICC	2765/2764
Foreign military (T)	ICC	1173/1173-1
Foreign national employee (U)	ICC	1173
DoD contractor – designated (E)	ICC	2765/2764
DoD contractor – not designated, but emergency essential or overseas (E)	ICC	N/A
Retired (R)	N/A	<b>2RET</b>
Reserve retiree (Q)	N/A	<b>2RESRET</b>
100% disabled American veteran (D)	N/A	<b>2765</b>
Former member - a 20-year active-duty serviceman who was eligible to retire but elected discharge (F)	N/A	<b>2765</b>
Transitional Assistance Management Program (F)	N/A	<b>2765</b>
Medal of Honor (H)	N/A	<b>2765</b>

<b>Member Category (Personnel Category Code)</b>	<b>CAC (ICC/Non-ICC)</b>	<b>Teslin Card (Form)</b>
Family Members – except children under 10	N/A	1173
Family Members – designated children under 10	N/A	1173

### 3 DEERS/RAPIDS Roles

The following information is discussed in this section.

1. What is a DEERS site ID?
2. What is a DEERS logon ID?
3. What is a VO/LRA?
4. What is an SVO?
5. What is an SSM?
6. What is a Project Officer (PO)?
7. What is the Role of the RAPIDS Workstation?
8. Where Do I Go for Help if I Have Questions About RAPIDS?

**Note:** The roles of Address Only Official and Read Only Verifying Official do not have card issuance privileges and are not detailed in this training guide.

---

#### 3.1 DEERS Site ID

A DEERS site ID is a unique six-digit number used to group a set of RAPIDS systems. End users, SPOs, and the D/R Ops Div also use a DEERS site ID to generate transaction reports by site. An example of a DEERS site ID is **102333**.

---

#### 3.2 DEERS Logon ID

Every user must have a valid CAC with associated PIN and a DEERS log on ID with associated password to use the RAPIDS application and access DEERS. RAPIDS is designed so that users must enter their own CAC and PIN to sign on to the system and to open records from DEERS. It is necessary to add the Windows log on account with a DEERS ID and password for each RAPIDS user at the site. Refer to *Section 5.3* of this training guide for detailed procedures. Initially, your DEERS Logon ID and DEERS password are distributed to you by mail, ensuring that no one else knows your DEERS password, **no exceptions**. The logon process lets the system know the users are authorized to use the application. All users must request a unique DEERS logon ID from the SSM. For security purposes, neither the password nor the PIN should be shared with anyone, including other VOs, SVOs, or SSMs. A VO should not log on to the RAPIDS workstation and allow another person to make updates. The VO should never leave his/her VO CAC unattended in the VO smart card reader/encoder.

### 3.3 Verifying Official

The DEERS VO performs the following tasks.

1. Adds, updates, retrieves, displays, transmits, and stores data on DoD sponsored individuals in the DEERS database after verifying the official documentation.
2. Generates the DD Form 1172 (Application for Uniformed Services Identification Card and DEERS Enrollment) and prints the DD Form 1172-2, (Application for DoD Common Access Card, DEERS Enrollment). **Note:** the DD Form 1172-2 will **NOT** be prefilled with sponsor information. The Sponsor must complete the form and have it verified by an authority of the sponsoring agency before the DEERS VO can add the sponsor to DEERS and produce a CAC. Verification authority procedures for the 1172-2 may vary between services.
3. Generates the CAC for the selected population and generates the teslin machine readable Uniformed Services Identification Card and select DoD Civilian ID cards for the remaining population of eligible individuals. Each sponsor CAC or ID card indicates the sponsor's status as Active Duty, Guard/Reserve, Retired, Civilian, Contractor, or Foreign National.
4. Suspends commissary, exchange, and/or Morale, Welfare, and Recreation (MWR) privileges, if necessary.
5. Notifies the PO or DMDC Support Office (DSO) when a purge, invalid entry, or lock to a record is necessary.
6. The VO is in a key position of responsibility and assumes the role of the LRA. The following are the VO's responsibilities regarding the LRA function of PKI. Many of the following are performed automatically through RAPIDS. These tasks are detailed in *Section 6* of this training guide.
  - Verify identity of card recipients as required by the AFI 36-3026(I).
  - Receive, verify, and enter card recipient information.
  - Use the RAPIDS workstation to issue the CAC, and to request certificates and download them to the CA prior to issuing to the card recipient.
  - Read and sign the DD form 2841, DOD (PKI) Registration Official Certificate of Acceptance and Acknowledgement of Responsibilities.
  - Provide the CAC recipient with and obtain his/her signature on the Subscriber Certificate Acceptance and Acknowledgement of Responsibilities forms (DD Form 2842). Ensure that users understand their responsibilities with respect to the CAC and the information stored on it.
  - Request that CAC recipients enter the PIN for their CAC.
  - Print the CAC.

- Update the CAC as necessary to reflect any change in the personnel category of the CAC recipient. This automatically issues/revokes certificates as needed.
- Terminate a CAC to execute revocation requests received from the LRA or other authorized sources.
- Assist in the management of the recipients' keys and certificates.

7. Comply with the security requirements (as described in the Security SOP for RAPIDS).

A VO may also have the role of a DEERS Issuing Official (IO), which allows signature privileges for the issuance of military ID cards. The VO has the ability to print the DD Form 1172 / 1172-2 and identification card. The IO name will appear (if selected) in the designated box on the DD Form 1172.

---

### **3.4 Super Verifying Official**

The DEERS SVO performs the following tasks:

1. Adds and maintains site specific information which is stored on the server database.
2. Generates reports that summarize the activities of the subordinate users, including all types of transactions and ID card types produced. Deletes report data as necessary to free up hard disk space on the server.
3. Performs DEERS SVO functions listed in *Section 8* of this training guide.
4. Ensures that all VOs have read and understand the "Message of the Day."
5. Notifies the PO or DSO when a purge, invalid entry, or lock to a record is necessary.
6. Comply with the security requirements (as described in the Security SOP for RAPIDS).

An SVO can be the Non-Commissioned Officer in Charge or the individual who takes on the supervisory responsibilities of the ID Card Section. The SVO is routinely a VO as well.

---

### **3.5 Site Security Manager**

The Site Security Manager is vital to the continued functioning of a RAPIDS site. A site cannot operate without an SSM that is physically assigned to work at that RAPIDS site location, functions as a RAPIDS user (VO) and is able to attend to all SSM duties and responsibilities. A limit of two SSMs per site, one primary SSM and one backup SSM, has now been enforced at all DEERS/RAPIDS sites. This limitation to two SSMs is primarily due to security changes within RAPIDS, a greater level of responsibility for SSMs in general, and accountability for Common Access Cards and related consumable materials. Sites having only one SSM should select and add a backup SSM.

Because this role is so important, DEERS requires two SSMs to be active for each RAPIDS site. Note that a site may not have more than two SSMs. The SSM is routinely as VO as well. Each

SSM is responsible for six key areas of operation:

1. User administration
2. CAC stock and consumables; ordering, management and accountability
3. Policy and procedure compliance
4. Site administration
5. Documentation and training
6. Use of the automated card management system (future enhancement)

Refer to *Section 9* for detailed information on SSM responsibilities.

---

### 3.6 Project Officer

Each Uniformed Service, its Guard and Reserve components, and some DoD agencies have an assigned PO. The DEERS/RAPIDS POs are responsible for service-specific policy, PKI policy questions, equipment relocation requests, requests for additional equipment, requests for initial access to DEERS or RAPIDS, Retiree Days/Open Houses, and approval for initial site ID requests. A complete listing of the DEERS/RAPIDS POs can be found in *Appendices C and D* of this training guide. A PO may perform the following operations.

1. Terminate a DEERS record for invalid entry with the assistance of the DSO Research and Analysis team.
2. Lock and unlock a family or person record.
3. Add the Dependent Abuse Personnel Entitlement condition to the sponsor record.
4. Approve requests for new DEERS site IDs, onsite RAPIDS training by FSRs, initial RAPIDS workstations, additional RAPIDS workstations, and RAPIDS workstation relocations for their Service.
5. Represent their Service's requirement to D/R Ops Div.
6. Provide policy guidance to their RAPIDS users.

---

### 3.7 Role of the RAPIDS Workstation

The RAPIDS workstation serves as the tool used to approve and issue certificates on the CAC and revoke certificates as necessary. The DoD PKI uses the RAPIDS workstation combined with the Issuance Portal as Registration Authorities to: (1) register DoD personnel who will receive the CAC with the CA, (2) create and print the CAC, and (3) download certificates to the CAC. The RAPIDS workstation will also support revoking certificates, resetting a user's CAC PIN, and backing up data from the CAC to DEERS. The CAC will be used for applications, such as

computer access, network access, e-mail encryption, building access, digital signature, and other functions as PKI applications are developed and deployed by the DoD.

New functionality and enhancements are built into RAPIDS to support the CAC.

1. Within the DEERS database, the DoD Electronic Data Interchange Personnel Identifier (EDIPI) has been established and can be used across computer systems as a unique identifier for an individual.
2. To support the issuance of e-mail encryption and digital signature certificates, RAPIDS collects e-mail addresses.
3. When terminating a CAC, RAPIDS captures the date of termination. This date will be used to revoke the certificates that reside on the terminated card.
4. The organ donor identifier is added to RAPIDS and prints on the Armed Services CAC.
5. The DD Form 1172-2 requests that card recipients identify the country to which they are assigned.
6. The Agency/Subagency for DoD civilians and DoD contractors is collected.

**Note:** The RAPIDS software produces the CAC. Separate applications must be written or procured by organizations that desire to use the CAC for building access and e-mail use. These separate applications are not detailed within this Training Guide. Contact your local command for guidance.

---

### 3.8 Responsibilities of the Card Recipient with Respect to PKI

A CAC Recipient's responsibilities include:

1. Use certificates and private keys only for official purposes.
2. Protect your private key and PIN from unauthorized use. Protect it as you would your bankcard.
3. Report any loss or compromise of your private key to the RAPIDS Issuing facility.
4. Comply with any policies established by the RAPIDS Issuing facility.
5. Read and sign the DD form 2842, DoD (PKI) Subscriber Certificate of Acceptance and Acknowledgement of Responsibilities.

The CAC is encrypted with PKI certificates that may be used for secure e-mail exchange, digital signature of documents, or security access.

---

### 3.9 Server and Remote Sites Responsibilities

A server site and its associated remote sites should always strive to maintain a good working

relationship and are encouraged to keep verbal communications open. Sites may be asked to sign an MOU/MOA between the points of contact (POCs) at the server/remote sites, which delineates these responsibilities and serves as a signed agreement for full cooperation of responsibilities between a server site and its associated remotes.

### **3.9.1 Server Site Responsibilities**

1. Assist remote sites in acquiring local incoming dial-up phone circuits to include coordination between the remote facility and the server base communications personnel. If applicable, obtain and maintain dial-up terminal server accounts/log on IDs from the base's terminal server administrator.
2. Coordinate with remote sites on operating schedules and planned system disruptions.
3. Notify remote sites when unscheduled disruptions occur, and work with remote sites to reestablish processing and communications links.
4. Download and install new RAPIDS software and notify the remote sites of the upgrade.
5. Provide access to the facility housing the RAPIDS server outside normal working hours, and/or leave the server system, operating as necessary to support remote sites.
6. Work with the remote sites when communications problems are encountered. This responsibility includes checking modem status. If the problem cannot be resolved locally, it is the responsibility of the server site to call the D/RAC / D/RSC-E / DSO-A for help.

### **3.9.2 Remote Site Responsibilities**

1. Obtain communication circuit(s) at the remote site location and the server location. Prepare and provide the funding for circuits at both sites.
2. Coordinate workstation operating schedules with the server site.

## 4 RAPIDS Help Resources

The following are various persons and sources to access for help regarding RAPIDS.

1. RAPIDS Web Resources
2. RAPIDS Online Help
3. RAPIDS Documentation on CD-ROM
4. D/RAC, D/RSC-E, or DSO-A, based on your site's location.
5. DEERS/RAPIDS FSRs
6. Your PO
7. Security Standard Operating Procedure for RAPIDS

---

### 4.1 RAPIDS Web Resources

DMDC invites all RAPIDS users to access the Verifying Officials Information System (VOIS) Web site. The VOIS provides RAPIDS VOs with quick and easy access to real-time systems information, up-to-date program information and many other resources such as archived Messages of the Day (MOTD), Points of Contact, links to other Web sites and more. To access the VOIS simply select **Tools|Web|VO Information System** from the RAPIDS menu.

From a non-RAPIDS computer, type, <https://www.dmdc.osd.mil/vois/owa/vois>. Our goal for this Web site is to provide instant systems status and current RAPIDS/CAC information to all RAPIDS VOs.

The Interservice Publication, AFI 36-3026(I), "Identification Cards for Members of the Uniformed Services, Their Family Members and Other Eligible Personnel" contains the policies supporting the DEERS and RAPIDS applications for the Army, Navy, Air Force, Marine Corps, Coast Guard, the Commissioned Corps of the National Oceanic and Atmospheric Administration (NOAA), the United States Public Health Service (PHS), and United States Armed Forces Reserve and National Guard. The instruction is used to prepare, issue, use, account for, and dispose of the Uniformed Services ID cards. The Interservice Publication is available on the World Wide Web (www) at <http://www.e-publishing.af.mil>. Type "36-3026" at the Short Title search text box and click "Go".

To request the Interservice Publication via Compact Disk - Read Only Memory (CD-ROM), at no charge, please contact:

SAF/AADD  
Bolling AFB, DC 20332-1111  
DSN: 754-2438  
Commercial: (202) 404-2438

OCONUS DSN Prefix: 312  
E-mail: [ets@pentagon.af.mil](mailto:ets@pentagon.af.mil)

The Air Force maintains an informative and helpful Web site for DEERS and RAPIDS issues. Go to <https://www.afpc.randolph.af.mil/deers> and view numerous policy topics, helpful tips and links to other resources. The DMDC Access Card Office (ACO) Web site provides useful information about the CAC. Go to <http://www.dmdc.osd.mil/smartcard> to log on and find CAC-related resources.

The Interservice Publication is being reformatted in an easy to read table format. Several common yet confusing topics are being rewritten in an easy to follow table format to help VOs interpret the proper answers to their policy issues.

All sites must have access to this publication. Compliance is mandatory.

---

## **4.2 RAPIDS Online Help**

The RAPIDS Online Help is designed to provide the basics of RAPIDS. It is not designed to provide the answer to every question that may arise while using the new RAPIDS.

RAPIDS Online Help can be found directly in your system while you work with RAPIDS. It is designed exactly like Online Help for Windows to make access quick and convenient. Refer to *Section 5.12* of this training guide for detailed instructions on using RAPIDS Online Help.

---

## **4.3 RAPIDS Documentation**

Your site has been provided a CD-ROM with various documents to assist you with the operation of your RAPIDS workstation hardware and software application:

- RAPIDS Training Tools
- RAPIDS Hardware Support documents
- Policy and Procedures
- RAPIDS Self-Help Relocation Guide

In addition, for RAPIDS policy questions, the Joint Service Publication AFI 36-3026 can be found at the Web site listed in *Section 4.1* of this training guide. These resources, along with the RAPIDS Online help, should be your first sources for answering questions pertaining to RAPIDS.

---

## **4.4 D/RAC, D/RSC-E, and DSO-A**

The D/RAC / D/RSC-E / DSO-A are points of contact for all users of the RAPIDS system providing expertise in the execution of the RAPIDS application as well as identifying, troubleshooting and resolving problems with RAPIDS system configurations, hardware, software and telecommunications. The D/RAC / D/RSC-E / DSO-A should be your first call when trying

to resolve problems or when you need assistance. A listing of phone numbers and addresses can be found in the Quick Reference Guide in *Appendix A* of this training guide.

#### **4.4.1 When to Contact the D/RAC / D/RSC-E / DSO-A?**

When in doubt as to who to call for help, contact the D/RAC / D/RSC-E / DSO-A. These Assistance Centers can help with any of the following concerns.

1. Questions about the RAPIDS application
2. Hardware failure: D/RAC / D/RSC-E / DSO-A will perform normal troubleshooting procedures to identify a hardware failure and contact the hardware vendor if appropriate.
3. Specific error messages received: When reporting problems involving opening RAPIDS, printing cards, encoding, saving to DEERS etc., it is very important for the VO to ensure that each problem is reported to the D/RAC / D/RSC-E / DSO-A with as much detail as possible. When a progress bar is displayed, note the progress bar status as well as the percentage reached. The status is often more important than the percentage. Report any error messages in detail. This will assist in troubleshooting any problems that occur.
4. Communications issues related to CAC, such as the CA server(s) is/are unavailable, or the RAPIDS site cannot reach the CAC Issuance Portal(s): D/RAC personnel would determine the problem by contacting the PKI Help Desk or troubleshooting the network. Network problems could encompass a site's LAN, local firewall configuration, WAN or within the DMDC network enterprise. D/RAC / D/RSC-E / DSO-A personnel will work with the DISN and local base communications personnel to resolve all communications issues.
5. CA Access Errors: A new RAPIDS VO/LRA has not been added to the CA Access Control List. D/RAC / D/RSC-E / DSO-A personnel will contact the PKI Help Desk to verify that the RAPIDS VO has been added to the CA Access Control List by involving DEERS Security personnel. DEERS Security personnel will refer the PKI Help Desk to the secure e-mail sent to add the specific RAPIDS VO to the CA Access Control List.
6. Card Errors: In this scenario, the RAPIDS CAC Status utility to read the certificate will be utilized to determine the status of the card. If the utility cannot read the certificates or access the applets, it will be assumed that either the card is damaged or there is a problem with the applets. The CAC will be reissued, and the certificate on the original card will be revoked through the RAPIDS software. Review the CAC return procedures in Appendix L of this Training Guide.

#### **4.4.2 When to Contact My RAPIDS Server Site?**

Contact your RAPIDS server site first if you are experiencing slow or no communications with the RAPIDS server or you have problems connecting via the modem or Virtual Private Network (VPN). Remote sites should inform their RAPIDS server site of non-hardware related problems first. Contact the D/RAC / D/RSC-E / DSO-A if the server site cannot assist in resolving the

problem.

---

#### **4.5 DEERS/RAPIDS FSRs**

The DEERS/RAPIDS FSRs are ready to assist users in the field with any RAPIDS application questions and training needs. Hardware and communications problems should continue to be reported to the D/RAC, D/RSC-E and/or DSO-A. FSRs are assigned regionally and assist the users with applications and onsite training. As explained in *Section 1.1*, your FSR is available to assist you in initial training for the RAPIDS application and follow-up questions. A copy of the FSR Regional Map is found in *Appendix B* of this training guide.

---

#### **4.6 Project Officers**

Each Service has a designated DEERS/RAPIDS Personnel and Medical PO who can answer any policy questions that you cannot answer by using the Joint Service Publication AFI 36-3026(I). All requests for new DEERS site IDs, new user log on IDs, RAPIDS equipment relocations, additional RAPIDS workstations, and new RAPIDS site equipment should be directed to your Personnel PO. A listing of POs by Service, with phone numbers and addresses can be found in *Appendix C* (Personnel POs) and *Appendix D* (Medical POs) of this training guide.

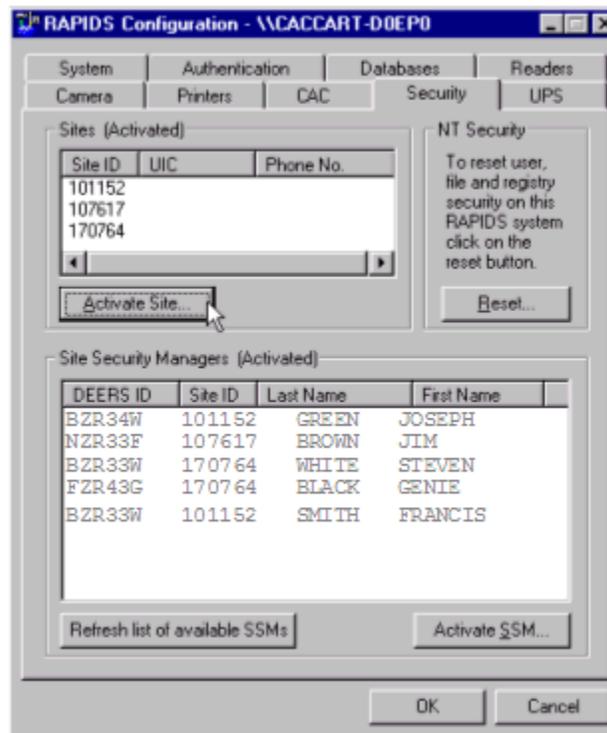
## 5 Becoming Familiar with RAPIDS

RAPIDS is a Windows-based application using icons, windows, menus, check boxes, and tabs for functions and navigation. RAPIDS application is designed to provide users with many choices on how to complete a single task. This section contains information needed to become familiar with the RAPIDS workstation. The menu, toolbar, help functions, and main screen views will be reviewed along with technical descriptions of each.

### 5.1 Activation of the Site and Site Security Managers

This segment details the required addition and activation of sites and SSM's to the CAC RAPIDS version 6 server. When an Installer or FSR issues the initial SSM CAC at the time of the initial RAPIDS CAC upgrade, the following procedure is required.

1. Log on to the Server as Administrator and open RAPIDS Configuration to the *Security* tab.



- Click on the Activate Site button and enter site number, UIC, and phone number to activate. This will add the site IDs to the Activated Site list.



Activate Site

Site ID: 170764

UIC:

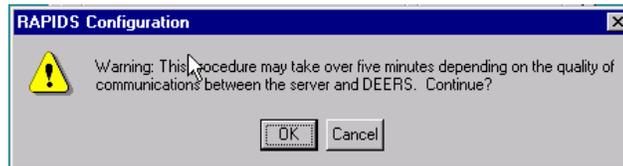
Phone Number:

OK

Cancel

Users for the new site will not be available until the transaction database is synchronized with DEERS.

- Refresh the SSM list to add the SSMs from the newly added sites to the Site Security Managers (Activated) pick list. The refresh can be performed at the server or the workstation.



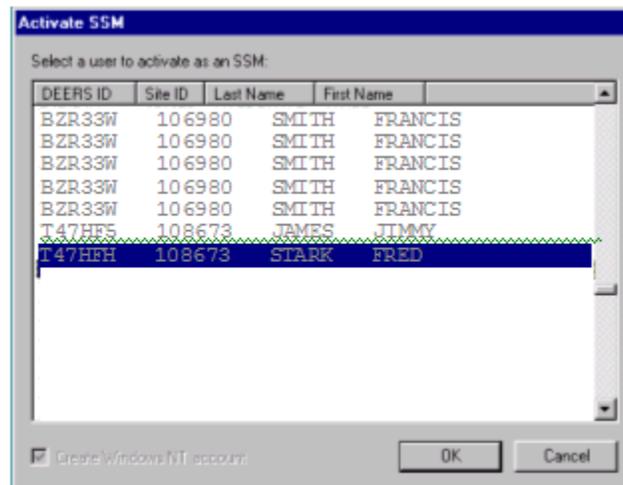
RAPIDS Configuration

Warning: This procedure may take over five minutes depending on the quality of communications between the server and DEERS. Continue?

OK

Cancel

- Once refreshed, select each SSM to activate.



Activate SSM

Select a user to activate as an SSM:

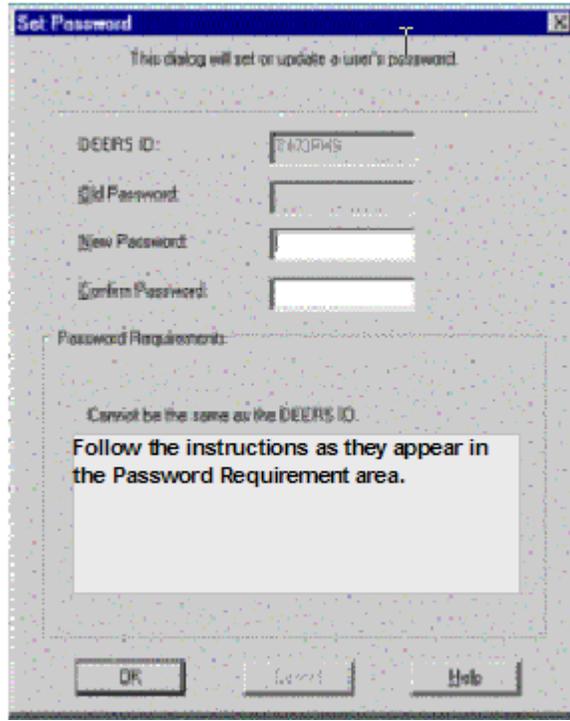
DEERS ID	Site ID	Last Name	First Name
BZR33W	106980	SMITH	FRANCIS
BZR33W	106980	SMITH	FRANCIS
BZR33W	106980	SMITH	FRANCIS
BZR33W	106980	SMITH	FRANCIS
BZR33W	106980	SMITH	FRANCIS
T47HF5	108673	JAMES	JIMMY
T47HH	108673	STARK	FRED

Create Windows NT account

OK

Cancel

5. Follow the instructions in the Set Password dialog box and the Password Requirements area to set your Windows Password. Windows will prompt the user to change this Password upon the first log on attempt.



**Note:** RAPIDS passwords are set to expire every 90 days. It will prompt you when it is necessary to change a password.



---

## 5.2 RAPIDS Passwords

To review and modify DEERS data, a RAPIDS user must use their DEERS (ACF2) logon ID and password or valid PKI Identity certificate on their CAC. All RAPIDS users must also have a Windows logon ID if they are to use RAPIDS. Most RAPIDS users will use their CAC to access RAPIDS and therefore are virtually unaffected by the Windows password. However, RAPIDS users that log on without a CAC must manage both the Windows and DEERS (ACF2)

passwords. To facilitate this process, logon information is stored for users on the RAPIDS server so that the user will only have to maintain the Windows password. When a RAPIDS user is prompted to change their password (every 90 days), RAPIDS will manage the synchronization of the DEERS (ACF2) password and the Windows password. This password is also stored on the VO's CAC for CAC/PIN logon.

The following sections discuss the setup of the Windows logon ID and password using the ActivCard Gold Utility.

---

### 5.3 Logging on to RAPIDS

RAPIDS logon activities are facilitated by the ActivCard Gold Utility. When the VO powers on a RAPIDS workstation or server, the ActivCard Gold log on replaces the usual Windows log on screen. The initial log on requires the VO to set his/her Windows login account and register his/her CAC Identity certificate with ActivCard Gold to allow future access to RAPIDS with their CAC. To do this, the VO must log on without the CAC inserted and use his/her DEERS ID and Windows password to log on. Once the VO has updated his/her CAC with the Windows Log on ID and password and has registered his/her certificate (as detailed in the following sections), the VO can use the CAC and PIN to log on to a RAPIDS workstation.

**No CACs should be left in either smart card reader/encoders when the VO is away from the RAPIDS workstation.** Sharing CACs or disclosing a PIN in order to accomplish VO/LRA duties is a serious security offense. Issuing a CAC under someone else's credential may result in all the CACs issued by holders of such cards having to be recalled and reissued by the site. It may also result in loss of position and such administration or other action as may be deemed appropriate by the local commander.

A VO should never log on to the RAPIDS workstation to allow another person to make updates nor should the VO leave his or her CAC unattended in the VO card reader. Your CAC contains your PKI certificates. A certificate is a computer generated digital record that ties a user's/entity's identity with their public key in a trusted bond. This trust is based on the individual's/entity's identity being verified and the certificates being created, signed, and issued by a trusted server.

All Verifying Officials must abide by all policy and procedures described in DoD Instruction 1000.13, the Inter-Services Instruction (AFI 36-3026(I), and the RAPIDS VO Certification Practice Statement (CPS).

**Note:** Establishing the connection with the RAPIDS server is dependent upon each site's communications infrastructure and varies between sites.

Each RAPIDS user, prior to logging in to the RAPIDS workstation with their CAC, must accomplish two tasks: (1) add the Windows Login Account and (2) register their ID certificate on the workstation. These steps are required for each individual user and must also be repeated for each new VO. To accomplish these tasks, each new VO must log on using their DEERS logon ID and Password. Certificates must be registered on each RAPIDS workstation that the VO will be using. The SSM may also register his/her certificates on the RAPIDS server, if one is

present at that site. An additional step of Adding Dial-up Settings may be necessary for users at workstations that are dialing into a RAPIDS server.

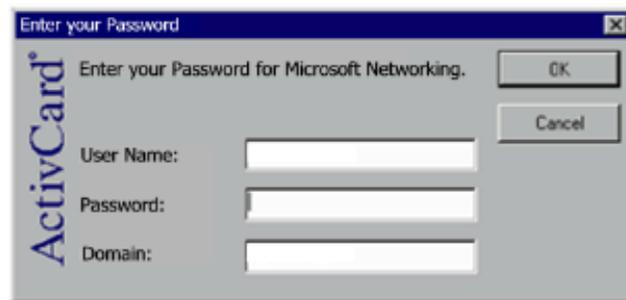
**Note:** If logging in with a DEERS user ID, the RAPIDS application will start automatically. Select the “Cancel” button on the RAPIDS progress meter before proceeding with the following steps. All users will need to complete these steps before they are fully functional as a RAPIDS VO.

There are two methods for logging into the RAPIDS version 6 workstation:

1. Login with logon ID and password (to be used for first time log on only).
2. Login with CAC and PIN (all subsequent logins).

### 5.3.1 First Time Login with Login ID and Password

First time users of a RAPIDS workstation must remove their CAC from the VO reader/encoder and enter their DEERS user ID and use their Windows password in place of their PIN as the two have not yet been associated through ActivCard Gold.



Once logged in, the VO must add a Windows NT login account through the ActivCard Gold application at any of the site’s workstations. This task is detailed in *Section 5.3.2* of this training guide.

### 5.3.2 Adding the Windows NT Login

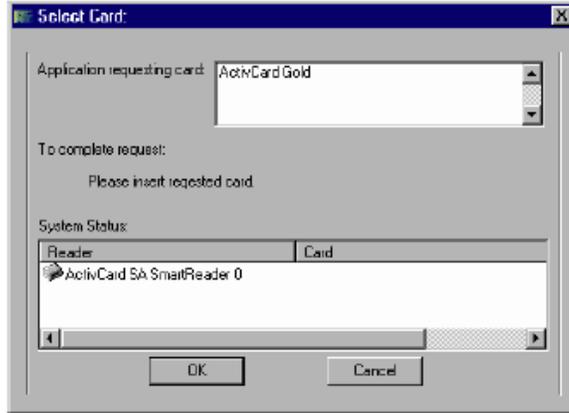
ActivCard Gold mediates access to the RAPIDS domain at each site. The VOs must add a Windows login account through the ActivCard Gold utility at any of the site’s workstations.

1. Insert the VO CAC into the VO reader/encoder. This would be the CAC for the VO logged on to RAPIDS.
2. Double click on the ActivCard Gold Icon in the System Tray.

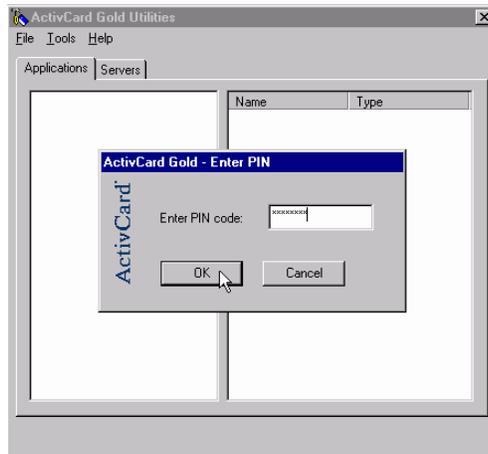


3. On occasion you may be asked to select which card reader your CAC is in. As a rule, when logging in, be sure that there is not a CAC in the card recipient reader/encoder.

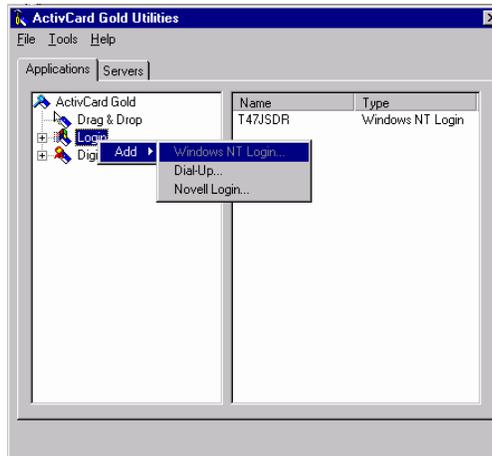
ActivCard names the VO CAC reader as “Smartreader 0” and the card recipient reader/encoder as “Smartreader 1”.



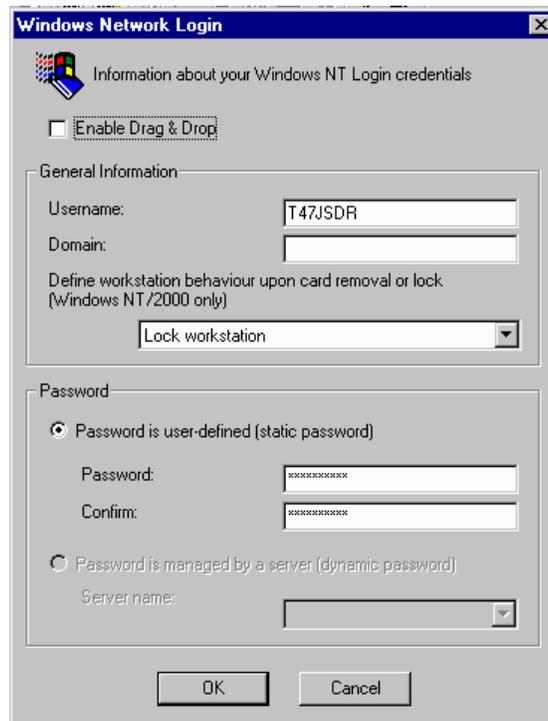
4. To add the Windows Login account so that VO can log on to Windows using his/her CAC, ensure that the VO’s card is inserted into the VO reader/encoder.



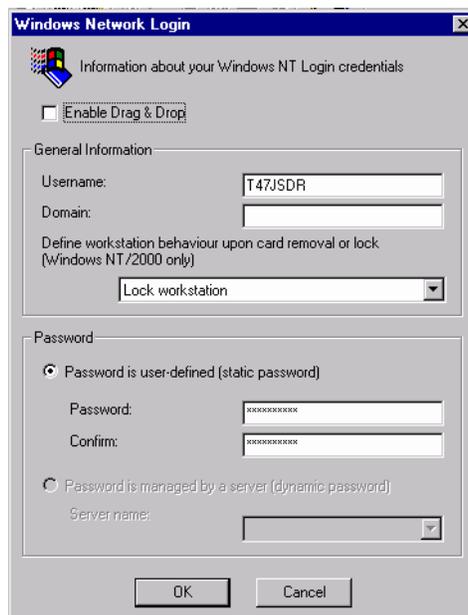
5. Right-click on the Login option in the left window of the ActivCard Application and select **Add|Windows NT Login** from the menus. This process needs only to be completed at one workstation connected to the RAPIDS server.



- At the Windows Network Login dialog box, type in the User Name (DEERS logon ID) in UPPERCASE. Input the RAPIDS domain name. This can be found by pressing CTRL+ALT+DELETE and reading it from the Windows Security screen. Verify that the option to “Define workstation behavior upon card removal or lock” is set to “Lock Workstation.” No other option is acceptable.



- The VO must enter and confirm their Windows NT password, and press **ENTER**. Once the log on settings are configured, follow the instructions in *Section 5.3.3* to register the VO's ID certificate.



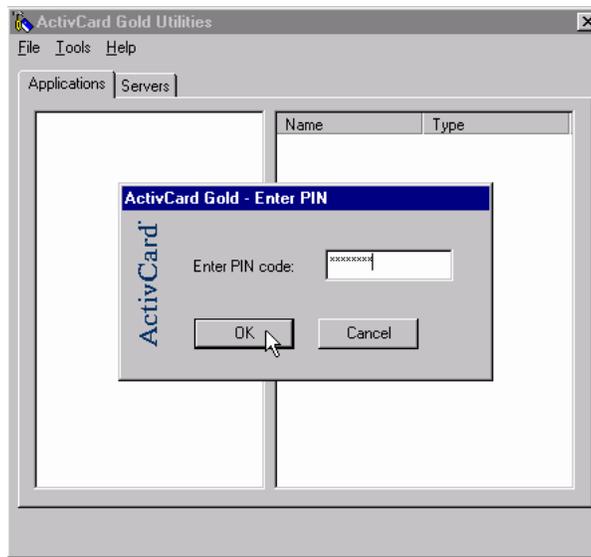
### 5.3.3 Registering Certificates

Prior to logging into RAPIDS, user must register their identity certificate to the RAPIDS workstation. This procedure must be performed at each RAPIDS workstation to which the VO wishes to log on. If you are already in the ActivCard Gold utility, skip to step 3.

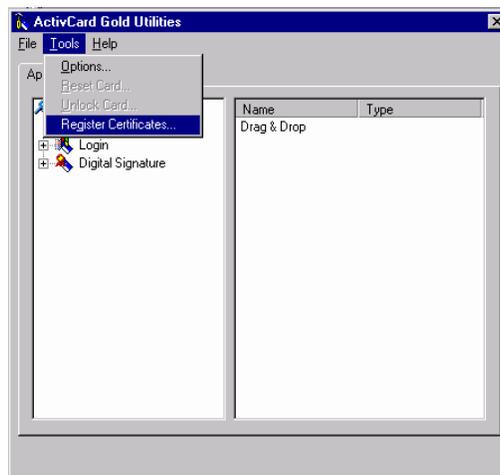
1. Insert the CAC that requires registration into the VO reader/encoder. This would be the CAC for the VO logged in to RAPIDS. Double click on the ActivCard Gold Icon in the System Tray.



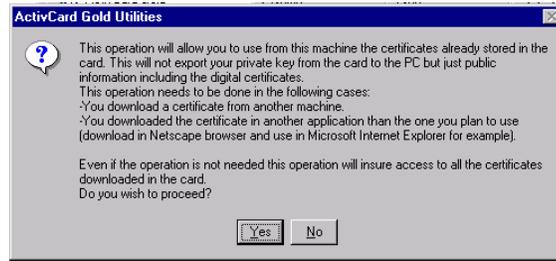
2. When prompted, enter the PIN for your CAC.



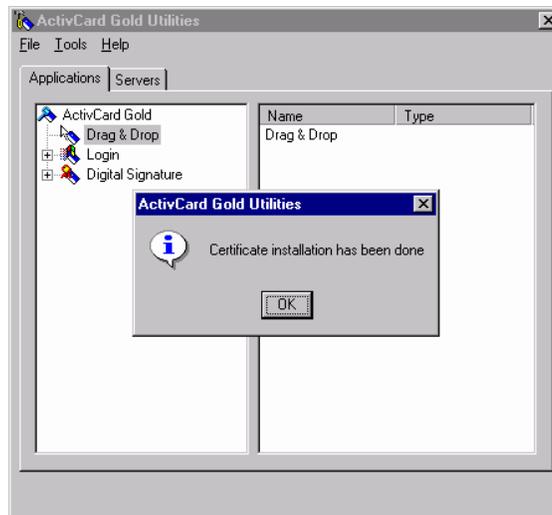
3. The RAPIDS user registers his/her certificate by selecting Register Certificates from the Tools menu.



The ActivCard Gold Utilities dialog informs the user that this action will allow you to use from this machine the certificates already stored in the card. Select **Yes**.



A confirmation message that reads, “Certificate installation has been done,” should appear. This registration process must be completed at each RAPIDS workstation for which the VO needs access.



---

## 5.4 Starting RAPIDS

After the RAPIDS user has (1) Added the Windows Login Account and (2) Registered the user’s certificate, he/she can start the RAPIDS application. A check to verify the VO’s identity certificate will be performed before allowing DEERS activity. DEERS will check and store the CA’s Certificate Revocation Lists to ensure that the VO’s certificate is still valid.

The VO should insert their CAC into the VO reader/encoder. Press CTRL+ALT+DELETE to display the log on screen. When prompted, enter the six to eight digit PIN associated with the CAC. Establish connection with the RAPIDS server. (This may vary depending on how each system is set up). If connecting from a dial-up site, it may be necessary to wait one to two minutes after the Windows desktop appears before proceeding to step two. A progress meter displays as the Windows desktop opens.



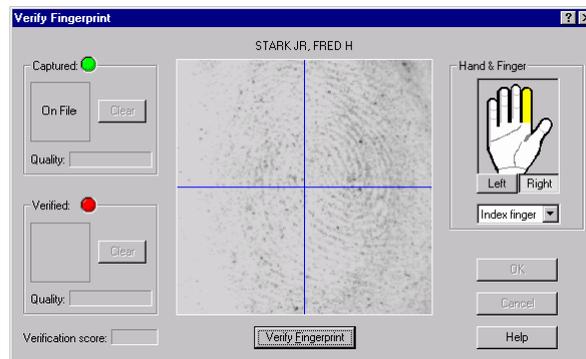
The RAPIDS application should start automatically. If the RAPIDS progress meter does not appear, double-click the RAPIDS icon. The application will display the RAPIDS logo while the computer starts the application. The VO will be prompted to select his/her certificate during the start-up process. Select Certificate and click **OK**.

If the VO has neglected to register their certificates on the RAPIDS workstation, RAPIDS will display a blank Client Authentication dialog box. Refer to *section 5.3.3* of this training guide.

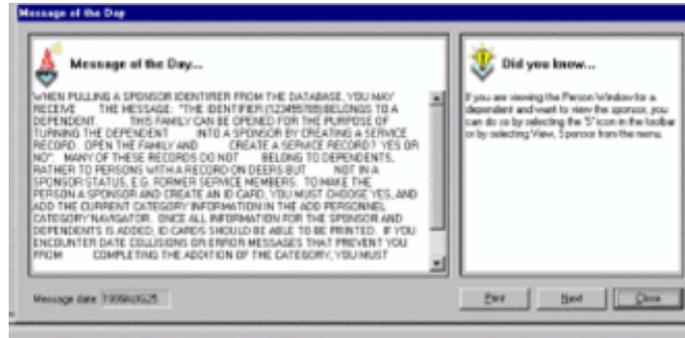


If more than a certificate displays, select the *View Certificate...* button to find the Identity Certificate. Do not select either of the e-mail certificates.

The VO will then be prompted to verify his/her fingerprint with the one stored on DEERS.



When the application has loaded the “RAPIDS Message of the Day” is displayed. When viewing the message for the first time, the “Message of the Day” will be highlighted in red. Print the Message of the Day by clicking **Print** in the dialog box. Click **Next** to allow the VO to scroll through tips and messages.



Open the VO (or other sponsor record) from DEERS or add the VO (or other sponsor) to DEERS. If a CAC was previously issued to the VO, RAPIDS will request that the CAC be inserted into the VO reader to verify e-mail certificates.

---

### 5.5 Security (Locking the RAPIDS Workstation)

RAPIDS security will lock a workstation that has been idle for five minutes. This security feature cannot be modified or removed by the end user.

When leaving your workstation for the day or for prolonged periods of time, close RAPIDS, log off of Windows and shut down the workstation. If leaving the workstation with the intent to return shortly, it is not necessary to exit completely out of the RAPIDS application unless a different VO will need to use the system. To lock the workstation in this case, remove the VO CAC from the system. If you logged in using the VO CAC, removal of the CAC will automatically lock the workstation. To unlock the workstation, the VO must re-enter his/her unique password or CAC PIN to access the application again. Never leave the immediate workstation area without first removing your CAC. Additionally, RAPIDS security will automatically lock a workstation that has been idle for five minutes, unless the system is in the process of encoding a CAC. If another VO will need access to your workstation, it will be necessary to exit the application and complete the following steps.

1. Exit Windows by clicking **Start** from the taskbar.
2. Select **Shut Down** from the menu.
3. Select the option button, **Close all programs and log on as a different user**. (If running Windows 2000, you will select **Logoff (User ID)**).
4. The new user of the workstation will then be prompted to input his/her VO specific information.

**WARNING:** You should not lock your desktop if you have updated your Windows password during that session. Instead, close RAPIDS and shutdown using steps 1-4 above.

RAPIDS SSMs should refer to *Section 9.2* for the steps necessary for SSMs to activate and select roles for RAPIDS users.

## 5.6 Opening a Family in RAPIDS

To open a family record in RAPIDS, the VO must have his/her CAC in the VO CAC reader and perform one of the following steps:

1. Select **File|Open Family From...DEERS database** on the menu bar.

-or-

Click the **Open Family**  icon from the toolbar.

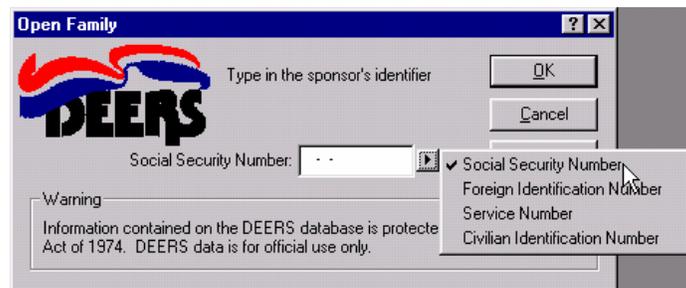
**Note:** The downward pointing arrow allows the user to select the location from which the family is opened.

2. Type the Sponsor's Identifier [the default identifier is the SSN].

-or-

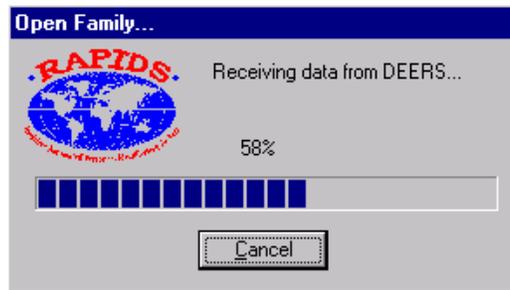
3. Use the bar code scanner to read the Sponsor's Identifier from the bar code on the sponsor/family members' current ID card. For a slot type scanner, insert the ID card/CAC with the Code 39 (one-dimensional) bar code down and facing the back of the scanner (side with the lettering and lights). Then, swipe the card through the scanner with a quick, smooth motion. For a laser type scanner mounted on a stand, hold the ID card/CAC with the Code 39 (one-dimensional) bar code facing up under the laser reading window of the scanner (the red laser beam should run across the entire length of the bar code) until it beeps, indicating a successful read.

**Note:** If the sponsor does not have a valid SSN, click the right pointing arrow next to the SSN field. A box will appear allowing the user to select from other Sponsor Identifiers, such as Service Number or FIN.



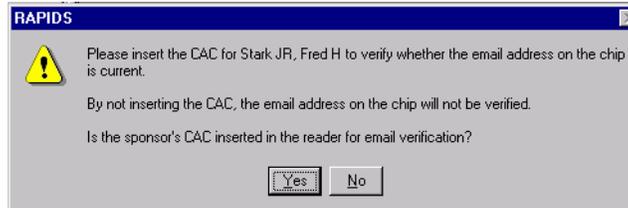
4. Select and enter the appropriate identifier and select **OK**.

When the appropriate identifier has been entered, the RAPIDS Open Family progress bar will display as shown in the following figure.



If the progress bar stops short of 100 percent, record the point at which it stopped, as well as the specific error message. This should be reported to the D/RAC / D/RSC-E / DSO-A.

If the sponsor that is being opened has been issued a CAC, RAPIDS will prompt the VO to insert the sponsor's CAC.



After successfully reaching 100 percent, the Family Tree window will appear listing all family records. To access a specific record, double-click the desired family member.

---

## 5.7 Taskbar and Taskbar Buttons

The taskbar is located across the bottom of the screen. Whenever a new program is started or another RAPIDS application window is opened, a button representing that program or application appears on the taskbar. These are called taskbar buttons. Click a taskbar button to switch to an open program or application window.

---

## 5.8 Notification Area

The notification area is the right side of the taskbar at the bottom of the screen that displays indicators dependent on the task being performed. The system clock and modem connections to the server are examples of indicators.

---

## 5.9 RAPIDS Menu

When the VO first opens RAPIDS, the menu bar is made up of the following items. Each item contains a drop-down list.

1. The File menu contains options of adding a new family, opening, or closing a family in DEERS. Once you have opened up a family, the options to save and print are enabled.

2. The Edit menu allows the options to undo, cut, copy, and paste information.
3. The View menu allows the user to turn on/off the family tree, family details, toolbar, and status bars. View also allows the user to change the active view (e.g., Address, Benefits, Characteristics, etc.).
4. The Tools menu allows an SVO to create and display error, ID card, periodic summary, and transaction reports. It also allows the RAPIDS SSM and SVO to update site information and remarks. It allows the RAPIDS SSM to configure devices and customize workspace preferences and allows for user administration.
5. The Window menu allows the user to arrange open windows and icons on the screen.
6. The Help menu offers RAPIDS Help, Windows Help, message/tip of the day, and information about the Privacy Act and RAPIDS software version.

Point and click each menu item to review the options it contains. When a family record is opened, the menu bar is expanded to include additional items as listed.

1. **View:** Allows the user to view Sponsor and dependent Address, Benefits, Characteristics, ID card, Coverage Plans, and Service Record views.
2. **Beneficiary:** Allows the user to update Address, Suspend Benefits, Medicare, Characteristics, DD Form 1172, ID card, and Service Record. Every command under Beneficiary affects a single-family member.
3. **Family:** Allows the user to add dependents, update addresses, create DD Forms 1172 and ID cards, verify family members, and lock/unlock record (available for POs only). Every command under Family will give the option to update multiple family members.

---

### 5.10 Quick Action Menu

The Quick Action Menu provides you with an additional way to perform certain tasks within RAPIDS. To open this menu, right-click the DEERS  icon, which is displayed at the top of the Family Tree whenever a family is opened.

The following options are included on the Quick Action Menu:

1. **Add Dependent:** Begins the Add Dependent Navigator.
2. **Update Address:** Begins the Update Address Navigator.
3. **Create DD Forms 1172:** Begins the Create DD Form 1172 Navigator.
4. **Create ID Cards:** Begins the Create ID Card Navigator.
5. **Lock/UnLock:** Allows POs and DSO to lock and unlock person records due to suspicion of fraud and abuse. A padlock icon appears in the Family Tree next to the name of any person whose record is locked. No updates can be made to the record.

6. **Verify:** Allows you to record the verification of a person's dependent status.
7. **Reopen Family:** Closes the family, with the option to save changes you have made to DEERS, and immediately re-retrieves the family information from DEERS.
8. **Print:** Prints a summary of the selected family member's address and phone number, characteristics and benefits.

---

## **5.11 RAPIDS Toolbar**

The RAPIDS toolbar contains the following items as icons:

1. New Family 
2. Open Family/Open Family From... 
3. Reopen Family 
4. Save View 
5. Save to DEERS 
6. Print 
7. Cut/Copy/Paste 
8. Toggle Family Tree 
9. Toggle Family Details 
10. Add Dependent 
11. Update Addresses 
12. Create DD Forms 1172 
13. Create ID Cards 
14. Update CAC 
15. Verify Dependents 

16. Non-context Sensitive Help 

17. Context Sensitive Help 

Each icon has tool tips available. Point the mouse to an icon to reveal the tool tip or point and click each tool item to review the options it contains. Some icons may be grayed or disabled, until a family is opened.

**Note:** When using the **Save to DEERS** command, the record continues to appear on the screen, but it is read-only. At this point, RAPIDS allows the VO to create a DD Form 1172 and an ID card for family members, but the VO cannot edit the record until it is closed and reopened. For this reason, it is a good practice to make all changes to the record before saving the record to DEERS.

If it becomes necessary to reopen a record after it has been saved, click the Reopen Family  icon on the toolbar while the record still appears onscreen. In the next few seconds, the progress monitor will indicate the status of the upload to DEERS and then the retrieval of the record from DEERS. When the Family record reopens, editing the data is allowed.

---

## 5.12 RAPIDS Help (Using Online Help)

While working in RAPIDS, Online Help is available for both Windows and for RAPIDS. There are several ways to access the Online Help; the best option depends upon whether the VO interested in specific tips for one particular item in RAPIDS or in a sweeping overview for first-time RAPIDS users.

Each unique screen of Online Help is called a Help topic. Longer help topics are too lengthy to be displayed in the Help window all at once and require the use of the scrollbar to read the topic. Hyperlinks (also called “hot links” or “hot text”) and the Back buttons in the top portion of the Help window, are available to help you move from one topic to another.

### 5.12.1 RAPIDS Help from the Menu

RAPIDS Online help within the RAPIDS application is found in the **Help** option under the RAPIDS menu. Help for the RAPIDS application is called Help Topics. This help option contains tabs entitled *Contents*, *Index*, and *Find*.

1. The Contents tab contains books that are arranged as chapters of a manual. Books are labeled according to the subject area that is covered by the book's contents. To see the contents of a book, double-click the icon that corresponds to the title you wish to open.
2. The Index tab contains an alpha/numerically sorted list of the topic titles and other key terms. To locate a particular topic, either scroll through the list of topics in the large text box, or begin to type the topic in the small, top box. As you type, the list will automatically scroll to find topic titles that match the characters you have typed.

3. The Find tab is the best tool to use when you can not find the Help topic(s) you need after having tried the Contents and Index tabs. It is designed to show you an exhaustive list of every Help topic that contains a particular word or phrase.

If a site would like to have a hard copy, Online Help can be printed two ways. The user may print each section under the **Contents** tab in Online Help separately (each topic will be printed on a separate page). Use the following procedures.

1. Select Help then Help Topics on the RAPIDS menu bar.
2. Under the Contents tab, various books (sections) are displayed. Click (highlight) the desired book and select Print.
3. As one book has completed printing (this will take a while), repeat Step 2 for each additional book under the Contents tab.

Selected sections of Online Help can also be printed through the following procedures:

1. Click Start; then select Programs|Accessories|WordPad.
2. At the WordPad desktop, select File|Open from the menu.
3. Online Help sections can be found in the directory:  
C:\ProgramFiles\DMDC\RAPIDS\Data\Document.
4. Open the desired section and select File|Print from the menu.

Other selections on the menu include **Message of the Day**, which allows the VO to view the message and tip of the day, and **Privacy Act**, which displays the Privacy Act Statement and the conditions applicable to sponsor or applicant.

It is important that the Privacy Act Statement be printed and posted in a common area for the VO and the card recipient to view.

### 5.12.2 Dialog Boxes and Dialog Tabs Help Button

All RAPIDS Navigators and some dialog boxes contain a **Help** button. Click **Help** to view the description of a RAPIDS dialog box or tab. When finished, click **Close** in the Help window.

### 5.12.3 RAPIDS Field Help

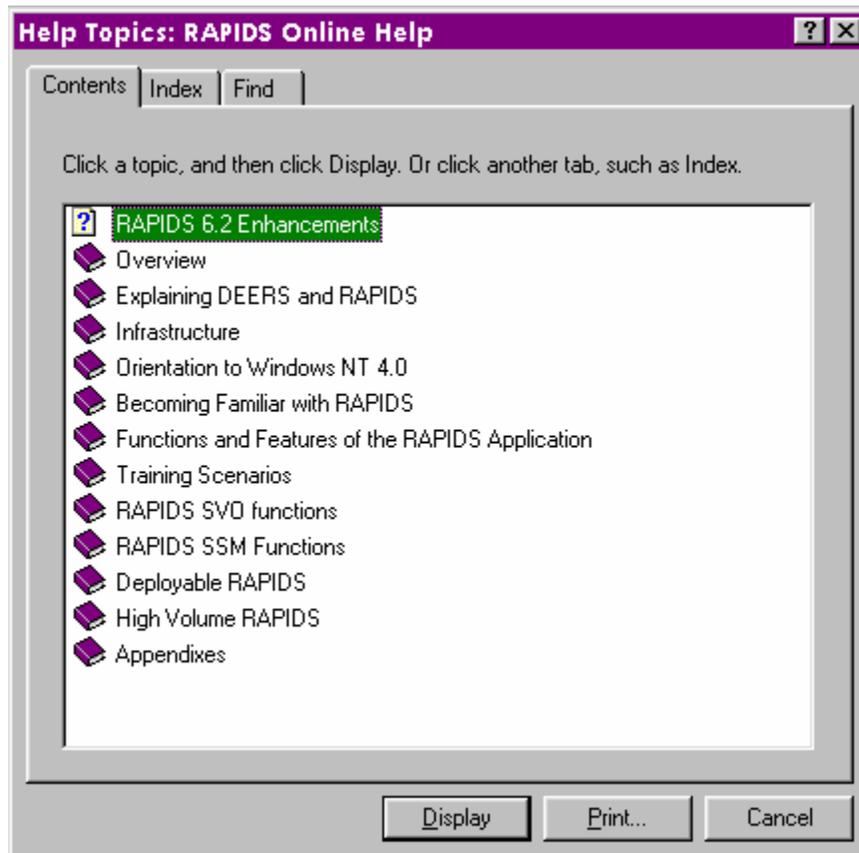


Whenever the user is within a field, press CTRL+F1 or click **Help** on the toolbar. Drag and drop the question mark to access information necessary to complete a particular field. A pop-up window displays general instructions for completing the field.

#### **5.12.4 Online Help Command Buttons**

1. The Back and Forward buttons are tools that maneuver forward and backward through the Online Help screens.
2. Back displays the previous topic the user viewed.
3. Contents displays the Help contents for the application, arranged by topic.
4. Find is used to search specific words and phrases in help topics instead of searching for information by category.
5. The Glossary is a listing of the definitions of certain terms contained in the RAPIDS glossary. Within the Online Help, these words have a dotted underline in the text. The definition of the term is viewed by clicking on the underlined word.
6. History displays a list of topics the user has accessed before.
7. Index allows the user to type a particular subject or word and receive information pertaining to that subject or word.
8. Navigator is a sequence of dialog boxes that appear sequentially in a predetermined order to guide the RAPIDS user through a multi-step task.
9. File|Print is used to print screens throughout Online Help.

### 5.12.5 Referring to RAPIDS Online Help



1. **RAPIDS 6.2 Enhancements:** This describes the updates done to the previous version.
2. **Overview:** Introduction to RAPIDS and DEERS, Functions of FSRs, Objectives and gives an overview of Help with Regulations.
3. **Explaining DEERS and RAPIDS:** Describes RAPIDS functions, features and enhancements, differences between DEERS and RAPIDS, and PKI.
4. **Infrastructure:** A detailed description of RAPIDS components, Issuance Portal, Information stored in DEERS/RAPIDS, CAC Architecture, DEERS/RAPIDS roles, discussion of workstation and server functionality and how to perform tasks particular to each, server and remote site responsibilities, contact information about the D/RAC / D/RSC-E / DSO-A.
5. **Orientation to Windows NT:** RAPIDS uses Windows NT as its operating system. This gives an overview of commonly used tasks like using a mouse, a keyboard, various components of a desktop, the window, dialog box, hot keys, locking the workstation and quitting windows.

6. **Becoming familiar with RAPIDS:** A detailed discussion of commands used by the RAPIDS application. This includes logging on to RAPIDS, RAPIDS Help, Information Views and their Contents etc.
7. **Functions and features of RAPIDS:** RAPIDS processing information guide and instructions for creating ID cards, DD Forms 1172, and related functions. Also details using Navigators, RAPIDS to issue the CAC and using the Tools menu.
8. **Training Scenarios:** Illustrates step-by-step instructions for common situations which the user may be faced when using RAPIDS.
9. **Using RAPIDS SVO Functions:** A detailed discussion of SVO functions, Site Information, and report processing information guide and instructions for completing various reports (e.g., audit trails).system and user security, users' definitions, privileges and responsibilities.
10. **Using RAPIDS SSM Functions:** Illustrates User administration, RAPIDS Configuration utilities and software distribution.
11. **Deployable RAPIDS:** A detailed description of RAPIDS systems configured as deployable.
12. **High Volume RAPIDS:** A detailed description of RAPIDS systems configured as high volume.
13. **Appendixes:** This contains the following:
  - Quick Reference Guide
  - Field Service Representatives Map
  - JUSPAC
  - JUSMAC
  - RAPIDS Acronyms
  - Privacy Act Statement
  - Procedures for moving RAPIDS Equipment
  - Site ID initial request (DEERS)
  - QWS3270 Emulator
  - Removing a card jam at the end of the Laminate Roll
  - Special Character Reference
  - Common Access Card and Consumables Order form
  - Card return Instructions and Form

### 5.13 Family Tree

A Family Tree is a hierarchical representation of a family. Branches of the tree can be expanded or collapsed by clicking on the plus (+) or minus (-) sign, or by double-clicking the desired file folder. The VO can change the width of the Family Tree by clicking on the splitter (vertical bar on the right side of the frame) and dragging it to the left or right. A Family Tree contains some or all of the following information and can be updated as needed. Each item in the tree corresponds to a data view that can be displayed in a person window.

The term dependent as it is used in this software application refers to a family member whose eligibility for entitlements is dependent upon his/her relationship to a sponsor.

**Note:** (*name*) refers to the name of the person selected within the RAPIDS application.

1. The **Address**  icon stands for “Address for (*name*).” When selected, an address view displays information such as street address, home e-mail address, effective date, and phone numbers.
2. The **Benefits**  (medical sign) icon stands for “Benefits View for (*name*).” When selected, the benefits view displays information such as Base Privileges, Civilian Health, Direct Care, or Suspensions.
3. The **Characteristics**  icon stands for “Characteristics of (*name*).” When selected, the Characteristics view displays Features and Sponsor Specific information, i.e., marital status, blood type, HIV/Panograph dates, organ donor status, and DNA sample dates. The information for dependents includes features, relationship, relationship condition, and student/incapacitated status.

**Note:** A VO may input blood type in a sponsor’s record if the field is blank or contains the incorrect information. Once this blood type has been confirmed (or corrected) by a medical reporting source, it will be locked and cannot be changed by a VO. Medical sources override personnel sources for blood type.

4. The **DD Form 1172**  icon stands for “DD Form 1172 for (*name*).” When selected, the previously created DD Form 1172 appears for the specified person. This icon may or may not appear under the Family Tree depending on whether or not a DD Form 1172 has been generated for this person during the session.
5. The **Card**  or **CAC**  icon stands for “Card for (*name*).” When selected, the previously created card information appears for the specified person. A view with tabs appears allowing the user to view information on the front and back, and characteristics and benefits associated with the card. This icon may or may not appear under the Family Tree depending on whether or not the card has been created. DEERS keeps a history of previously printed cards which are displayed with a faded icon.

6. The **Other Contract Plans**  icon stands for “Other Contract Plans for (*name*).” When selected, the insurance view appears displaying information such as Other Government Programs (Medicare), Delivery Program (TRICARE Prime), or Dental Premium information.
7. The **Service Record**  icon stands for “Service Record for (*name*).” When selected, the Service Record view appears displaying information such as Personnel Category, Personnel Condition, Work E-mail Address, Branch, Rank, Pay Grade, and Other. This icon will only appear for sponsors.

Click each tab to review the options it contains. Also, toggle the Family Tree on/off by selecting **View** and **Family Tree** from the menu bar to hide/unhide the Family Tree window. As you click the right mouse button on each item in the Family Tree, you will receive a separate context menu of commands that are specific to the item you right-clicked on. Everything normally found in the **Beneficiary** and **Family** menus can be accessed using this approach. Users are encouraged to take advantage of this feature. It will reduce wasted time hunting through menus and/or opening Person windows and searching for command buttons.

---

## 5.14 Family Tabs

The **Family** tabs are located on the bottom of the RAPIDS screen. These tabs include **Tasks**, **Tree Details**, and **Sponsor Confirmation** information.

### 5.14.1 Tasks Tab

The **Tasks** tab contains a list of prioritized tasks that should be completed before the user saves changes in DEERS. Each task is listed with an icon representing its priority, the person for whom the task should be completed, and a brief description of the task. The **Tasks** tab assists users by providing a starting point when they open a family. It serves as a checklist to ensure all family data is current with one save transaction.

The following icons represent the three task priority levels:

1. **Required (Red)** : The user must complete this task before information can be saved to DEERS. (Example: The existence of invalid information or colliding personnel category segments).
2. **Recommended (Yellow)** : The user is advised to complete this task before saving information to DEERS. (Examples: Verify dependent, capture fingerprint).
3. **Informational (White)** : The user is not notified that this task exists before saving information to DEERS. The task is considered low priority. (Examples: Enter hair color, enter weight).

When a user completes a task, it is removed from the Family Details dialog bar. Double-click on the item in the task list or invoke the appropriate command from the main menu or toolbar to complete a task.

### 5.14.2 Tree Details Tab

The *Tree Details* tab allows the VO to view sponsor or family member data without opening another window within the Person window. The data it contains depends upon which icon is highlighted in the Family Tree, as indicated below.

Information view Highlighted in Family Tree	Data Displayed
Address	Current address and ZIP + 4, address effective date.
Benefits	Category or relationship, condition, benefit dates, and the status of commissary, exchange, and MWR benefits.
Characteristics	SSN or other PIN, dependent relationship, relationship condition, date of birth, relationship dates, and last verification date.
Other Contract Plans	Program and effective dates.
Service Record	Category, condition, and service record dates.
E-mail	Work E-mail Address

### 5.14.3 Sponsor Confirmation Tab

The *Sponsor Confirmation* tab allows you to view the confirmation date and confirmation status of selected sponsor information. Confirmation of information takes place on the DEERS database, when information entered into DEERS via RAPIDS is compared with the authoritative data provided to DEERS by the sponsor's Service. DEERS receives daily and weekly electronically transmitted data from the Services as well as tapes.

When differences appear between the RAPIDS originated data and the information on the Service tapes, both data values are stored on DEERS, and the RAPIDS originated data is shown when you pull the information up on RAPIDS.

The first two columns of information display the description and value for the sponsor. Then, for each sponsor personnel category, a row is displayed that indicates the confirmation date and confirmation status for the effective date, unit identification code (UIC), and pay grade.

1. **Confirmation Date:** The date at which the data entered into RAPIDS is compared to the data on the authoritative Service tape.
2. **Confirmation Status Codes:** The following are status codes and their meanings.
  - **Verified:** The information entered into DEERS via RAPIDS is found to match the information on the Service tape. Project Officers and Field Service Representatives do not have the privileges to terminate data verified by the Service Master Files.

- **Unverified:** The information entered into DEERS via RAPIDS has not yet been checked against the Service tape.
- **Not Verifiable:** This item of information is not stored and cannot be verified. Suspense exists because DEERS receives data for a sponsor from more than one source. However, some populations have only one source (that is, Foreign Military, dependents). These single source populations do not require verification and are not verifiable.
- **Discrepant:** This item of information is different from the information on the authoritative Service tape. If information shown on RAPIDS differs from documentation provided by the sponsor, it may be necessary to call the SPO or DSO for resolution.

---

### 5.15 Person Window

When Address, Benefits, Characteristics, Coverage Plans, or Service Record is accessed from the Family Tree, the appropriate Person window is displayed. The Family Tree icon can appear as , which indicates that the sponsor's document window is currently open; or as , which indicates that a dependent's document window is currently open. The type of window accessed will appear in the title bar with the name of the person. Some fields are read-only (grayed) and some fields allow the user to make changes. The following illustration indicates the Person Toolbar, Title Bar, Fields, and Tab on the Address Person View.

The **Person** toolbar may contain the following icons, (see icons in the Family Tree).

1. Address
2. Benefits
3. Characteristics
4. DD Form 1172
5. Card
6. Other Contract Plans
7. Service Record(s)

These views vary according to the category and condition of the sponsor or dependent.

Dependents' document windows have a  (Sponsor button) which, when clicked, opens the sponsor's document window to the same view as the view shown in the dependent's document window.

## 6 Using the RAPIDS Application

This section explains the major functions of RAPIDS and the navigators and viewers used to perform these functions. The user will learn how to differentiate between a category and a condition and be introduced to special features used to customize each workstation.

---

### 6.1 Navigators

The RAPIDS application simplifies transactions for its users by using navigators. In RAPIDS, navigators are sets of dialog boxes, arranged in a particular order, that guide the user step-by-step through data processing tasks. Navigators are capable of skipping steps or adding steps where indicated as applicable DoD policy varies for the individual being processed. Navigators deliver many of the benefits of a rule based software system such as RAPIDS. Some of the most commonly used navigators are listed below. Most navigators have Continuation Options. If the user selects a continuation option, he/she is guided through that task without having to go back to the menu to invoke the operation. These Continuation Options allow the user to select the Continuation Options that should be selected by default for each navigator.

#### 6.1.1 Open Family

When selecting **Open Family From**, in the RAPIDS File menu, a drop down list of alternative sources from which to reference a family is displayed. These sources are **DEERS Database**, **Offline Repository**, **PDF417 Bar Code**, and **Mass Issue Repository**.



### 6.1.2 Add Sponsor Navigator

The *Add Sponsor Navigator* adds a sponsor to the DEERS database.

1. Select **File** on the main menu and **New Family** from the drop-down list.
2. Type in the Sponsor’s Identifier (the default identifier type is SSN). If the sponsor does not have an SSN, click on the arrow next to the SSN field. A box appears, allowing the user to select from other identifiers. (Refer to *Section 6.10* of this training guide for further detail on alternative identifiers). Select the appropriate identifier and then click **OK**.
3. The Add Sponsor Navigator dialog box appears. The Add Sponsor Navigator has the following Continuation Options: Add Personnel Condition, Add a Dependent, Add Personnel Category, Issue a DD Form 1172/1172-2, and Issue an ID card.
4. The navigator guides the user through the steps to complete the selected operation. Select **Finish** when all information is complete.
5. The Add Sponsor Summary screen appears when all screens have been completed for a sponsor record. The user has the option of modifying the information or creating the sponsor. To make changes to any information listed on the summary page, click **Modify** to page back (in reverse order). When an error occurs, the application will alert the user.
6. Select **Create** to complete the navigator.

### 6.1.3 Difference between a Personnel Category and a Personnel Condition

It is important to know the difference between a category and a condition. A Personnel Category represents the way in which a DoD personnel or finance center views the sponsor, based on accountability and reporting strengths. Personnel Conditions occur within a Personnel Category and affect the person’s entitlements or privileges. A sponsor may have more than one Personnel Category, with multiple Personnel Conditions associated with each Personnel Category.

A family member will have a Relationship Category and may have one or more Relationship Conditions (see *Section 6.1.4* training guide). Only certain conditions are available for certain categories. When a category/relationship is terminated, it displays a red **X** in the family tree. This alerts the user that this category/relationship has been terminated.

#### 6.1.3.1 Personnel Categories and Their Related Conditions

Category	Applicable Conditions
Academy Student	[None]
Active Duty	Appellate Leave Military Prisoner POW/MIA

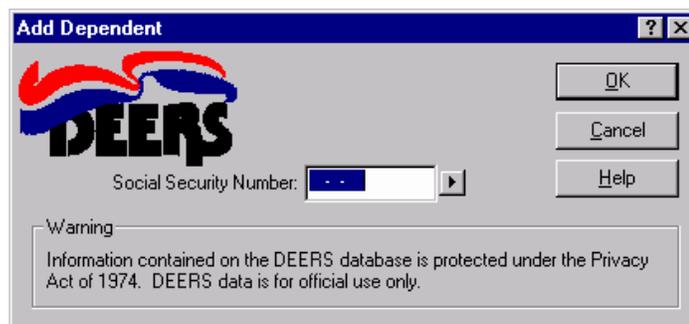
<b>Category</b>	<b>Applicable Conditions</b>
Disabled American Veteran	[None]
DoD Civil Service	Non-CONUS Assignment Living in Guam or Puerto Rico Living in Quarters Emergency Essential-overseas only Emergency Essential-CONUS Emergency Essential-CONUS/living in quarters
DoD Contractor	Non-CONUS Assignment Living in Guam or Puerto Rico Emergency Essential-overseas only
DoD Non-Appropriated Fund Employees	[None]
Foreign Military	DoD Sponsored in US DoD Non-Sponsored in US DoD Sponsored Overseas
Foreign National Employee	Emergency Essential-overseas only
Former Member	Granted Retired Pay
Lighthouse Service	[None]
Medal of Honor	[None]
National Guard	On Active Duty Appellate Leave Military Prisoner POW/MIA TA-30
Non-Government Agency Personnel	Non-CONUS Assignment Living in Quarters
Other Government Agency Contractors	Emergency Essential-overseas only Emergency Essential-CONUS Emergency Essential-CONUS/living in quarters Living in Guam or Puerto Rico Living in Quarters Non-CONUS Assignment
Other Federal Agency Employees	Emergency Essential-overseas only Emergency Essential-CONUS Emergency Essential-CONUS/living in quarters Living in Guam or Puerto Rico Living in Quarters Non-CONUS Assignment

Category	Applicable Conditions
Reserve	On Active Duty Appellate Leave Military Prisoner POW/MIA Selective Reserve Separation TA-30
Reserve Retiree	On Active Duty
Retired	On Active Duty TDRL to PDRL

### 6.1.4 Add Dependent Navigator

The  *Add Dependent Navigator* is used to add a dependent to the DEERS database. If Add Dependent was selected from the *Add Sponsor Navigator Continuation Options*, the *Add Dependent Navigator* will automatically appear after the sponsor's *Navigator Summary*. RAPIDS then searches DEERS for the existence of the person identifier specified when an attempt is made to add family members or change the identifier of an existing family member.

1. Select **Family** on the main menu and **Add Dependent** from the drop-down list.
2. The Open Dependent dialog box (similar to the Open Family dialog box) appears. Type the dependent's identifier type (the default identifier is the SSN). If the dependent does not have a valid SSN, click on the arrow next to the SSN field. A box appears allowing the user to select from other identifiers. Click **OK**. If a Person ID is entered, a DEERS search is conducted. If the new family member is already on DEERS, RAPIDS will populate the navigator with that person's information.



3. The navigator guides the user through the steps to complete the selected transaction. Select **Finish** when all information is complete.
4. The Add Dependent Summary screen appears when all screens have been completed for a dependent. The user has the option of modifying the information or creating the dependent. To make changes to any information listed on the summary page, click **Modify** to page back (in reverse order).

- If **Add Dependent** was selected as a continuation option at the Add Dependent Navigator, the Add Dependent Navigator will appear again after the summary. Continue with the process until all dependents have been added to the DEERS database.

-or-

If **Add Dependent** was not selected, additional dependents can be added by selecting **Family|Add Dependent** from the menu.

- After all dependents have been added, select **Create** to complete the process.

The following table lists valid RAPIDS Relationships and their applicable relationship conditions. By adding a relationship condition, the dependent’s benefits or eligibility dates could change to reflect appropriate benefits.

Relationship	Relationship Conditions
Child	Lives with entitled Former Spouse Sponsor provides over 50% Support Less than 50% Support Accompanying Sponsor Terminate entitlement under Sponsor
Former spouse	[None]
Parent	Accompanying Sponsor
Parent-in-law	[None]
Spouse	Accompanying Sponsor Terminate entitlement under Sponsor
Stepchild	Lives with entitled Former Spouse Sponsor provides over 50% Support Less than 50% Support Accompanying Sponsor Terminate entitlement under Sponsor
Stepparent	[None]
Ward	Court Order/Pre-adoptive Lives with entitled Former Spouse Sponsor provides over 50% Support Less than 50% Support Accompanying Sponsor

The **Modify** button allows a VO to change a dependent’s SSN. When selected, this option searches DEERS for the SSN entered. If DEERS finds that the SSN that the VO is attempting to change exists elsewhere on DEERS, RAPIDS will prompt the VO to end entitlements under the current sponsor.

### 6.1.5 Update Address Navigator

The  *Update Address Navigator* allows the user to update the address for the entire family or

individual family members. Legislation (Section 363 of the Personnel Responsibility and Work Opportunity Reconciliation Act of 1996) requires the sponsor to provide a new address for DEERS within 30 days of a move.

**Note:** When retrieving an existing family record into RAPIDS, the VO should verify the address, telephone number, and e-mail address information for the sponsor and each dependent (as applicable), making corrections as necessary, before performing other tasks, such as creating the DD Form 1172 or ID cards.

1. From the RAPIDS menu, select **Family|Update Address**.
2. When a VO selects the **Address Navigator**, the following options appear.
  - Enter a new address for one or more family members.
  - Copy an existing address to other family members.
  - Copy an existing address to all family members.
3. The navigator guides the user through steps to complete the selected update. The address screen displays the current address and phone numbers. Make changes as required. Enter the correct effective date of address whenever possible.
4. Select **Finish** when all information is complete.
5. The Update Address Summary lists the family members who will be updated with the new address. To make changes to any information listed on the summary page, click **Modify** to page back (in reverse order) or select **Update** to update the address.

### 6.1.6 Suspend Benefits Navigator

The *Suspend Benefits Navigator* allows any VO to suspend Medical, Commissary, MWR, and Exchange privileges for an individual.

1. Select the family member in the Family Tree whose benefits are to be suspended.
2. From the RAPIDS menu, select **Beneficiary|Suspend Benefits**.
3. Complete the following data. Use check boxes, combo boxes, or type in text as applicable.
  - Benefit(s) to be Suspended
  - Suspension Begin and End Dates, or Unknown
  - Reason the Benefit is Being Suspended
  - Person initiating this Suspension
4. Select **Finish** when all information is complete.
5. The Suspend Benefits Summary lists the family member who will have benefits suspended and benefits suspension information. Select **Create** to save the changes.

**Note:** This function should only be used for those beneficiaries who have abused their benefits or for whom a Direct Care suspension is required as directed by SPOs. The following are reasons for suspension of Direct Care (Medical).

- Refusal to provide SSN
- SSN not provided after first grace period

A relationship condition of “Sponsor provides over 50% Support” should be added to children not residing with the sponsor and not entitled to commissary benefits due to a “Divorced” status. In addition, no condition or suspension of benefits should routinely be added to those children under the age of ten.

### 6.1.7 Verify Dependents

The  *Verify Dependents* tool was created to verify/update dependents' eligibility information. The VO puts a check mark in the check box next to family members that are being verified by the sponsor. This tool allows family members to have an ID card produced (within 90 days of the verification) by any RAPIDS site without being accompanied by the sponsor.

1. The current use of this feature should be to verify with the sponsor which family members are eligible and to verify each family member. The user should only check the boxes of the family members who have been identified as eligible by the sponsor.
2. The Joint Uniformed Services Personnel Advisory Committee (JUSPAC) has not yet written the official policy for use of the electronic verify option in place of the DD Form 1172. The issuing site must note that current regulations still require a pre-verified or notarized DD Form 1172 to be presented at the issuing facility for receipt of an ID card.
3. The dependent's ID card expiration date will be up to four years from the date the sponsor verified the dependent, not four years from the date the ID card is issued.

### 6.1.8 DEERS/RAPIDS Fingerprint Capture Process

The *Fingerprint Capture* dialog allows the user to capture a fingerprint for all sponsors processed by RAPIDS. A fingerprint is required when all of the following conditions are met.

1. The workstation is equipped with a fingerprint scanner.
2. The card recipient is either Active Duty, Guard/Reserve military personnel, Retiree, survivor receiving annuity payments derived from the service of a deceased person (URW), or any sponsor receiving a CAC issued through RAPIDS.
3. The person is being issued an ID card or no recent fingerprint is on file as indicated by RAPIDS.

RAPIDS VOs will not capture fingerprints for any family members except widows. Disabled Veterans are not required to have fingerprints captured. The fingerprint data will be transmitted

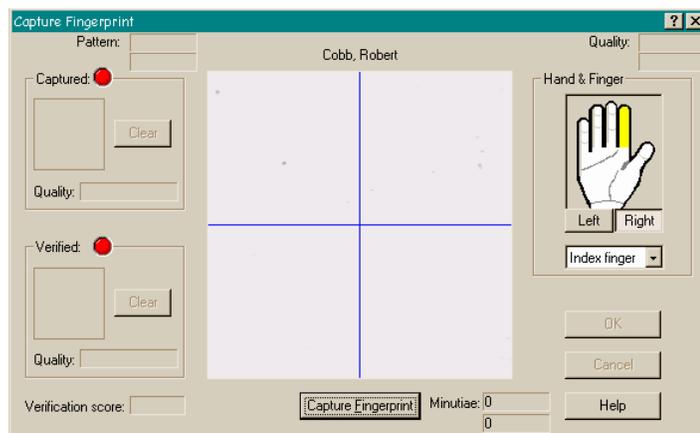
to DEERS using a process similar to the transmission of photographs. This transaction currently occurs after a completed ID card transaction and when the family is saved to DEERS.

In RAPIDS, when producing a CAC, RAPIDS will ask the VO to match the sponsor's fingerprint with the fingerprint stored on the DEERS database. Considerable enhancements have been made to the quality of the fingerprint captured. These enhancements increase the chances of a positive match when a biometrics match is required. When a fingerprint in DEERS is in the old format, the RAPIDS application will capture and send the new fingerprint format to DEERS.

If a fingerprint match fails, the VO has the capability to override a failed fingerprint match provided the card recipient has presented sufficient documentation for the VO to verify their identity. All decisions by a VO to override a failed fingerprint match are audited.

Fingerprints are captured using the following procedure.

1. Open **Sponsor**.
2. Open **Characteristics** view.
3. Select the **Fingerprint** tab.
4. Click **Capture...**
5. The RAPIDS *Capture Fingerprint* dialog box appears as shown below.



6. The default fingerprint captured should be the right index finger. This can be altered if necessary by selecting the hand and finger used from the upper right hand side of the Capture Fingerprint dialog box. Position the individual's right index finger on the fingerprint scanner. Notice that the fingerprint is now displayed on screen. Ensure that the core of the fingerprint is centered and not skewed (tilted to one side) by moving the positioning of the finger on the scanner.
7. Click on **Capture Fingerprint**. If a good quality print is captured, a green light appears in the upper left side of the dialog box. If a red light appears, recapture the fingerprint by clicking **Capture Fingerprint** again.

8. Verify the fingerprint by first removing the finger from the fingerprint scanner and then positioning the same finger on the fingerprint scanner. Click **Verify Fingerprint**. A green light appears in the middle left side of the dialog box if a good quality print is captured. If a red light appears, recapture the fingerprint by clicking **Verify Fingerprint** again.
9. Select **OK** to continue.
10. The sponsor's Characteristics view will now display the fingerprint, the date the fingerprint was taken, and the finger displayed.
11. RAPIDS will prompt the user the next time it is necessary to capture the individual's fingerprint.

In rare instances, it may be impossible to capture a person's right index fingerprint, and it may be necessary to try a different finger. Age, medication, and stress may also affect the quality of the fingerprint. After three failed attempts, the application allows you to proceed without capturing a fingerprint by clicking **Cancel**. The message, "Problem with fingerprint image quality. Empty," appears after each failed attempt. Click **OK** and proceed.

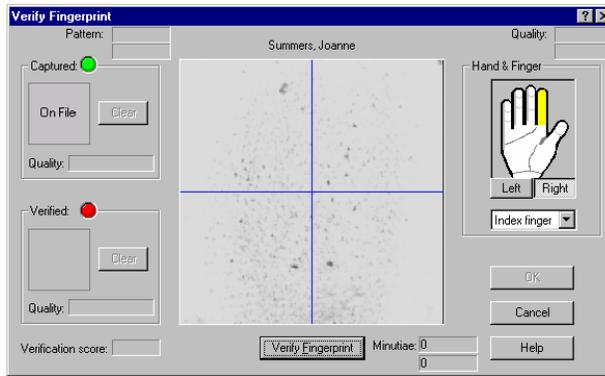
The verification of fingerprints for all VO's must be performed before starting RAPIDS to issue CACs. To facilitate VO fingerprint validation, the fingerprint reader can be configured to read VO fingerprints upside-down, so the fingerprint reader will not have to be physically moved for each VO log on. Select **Tools|Configuration|Readers**, then chose Rotate VO Image.

The lens cleaning cloth and PreScan formula are very important for the upkeep of your fingerprint scanner. The cleaning cloth provided by the vendor should be the only cloth used to wipe the surface of the fingerprint scanner. Paper towels and tissues should never be used. In most cases, the residual print you see on the platen will not affect the next fingerprint. It is only necessary to clean the platen when you notice residue on the Capture Fingerprint dialog box on the screen. The platen surface is extremely fragile and it might be necessary to remind card recipients to remove any jewelry that may scratch the platen during the fingerprint capture process. The PreScan formula should only be used on persons with poor skin conditions and especially dry skin to enhance the definition of the finger ridges prior to scanning. The PreScan should only be used after one or more attempts to capture the fingerprint have failed. It should not be used routinely for all card recipients, as it will leave a deposit on the fingerprint platen.

### 6.1.9 Bypass Fingerprint Capture Navigator

Sponsor fingerprints are required in current RAPIDS to issue a CAC. However, individuals with no fingers or illegible fingerprints can be issued a CAC using the **Bypass Fingerprint Capture** navigator and the SSM's digital signature to authorize the bypass. If the VO issuing the CAC is a SSM, a second SSM will be required to authorize the bypass. The SSM will be prompted to enter their CAC into the second (recipient) reader. The system will require the SSM to enter their PIN.

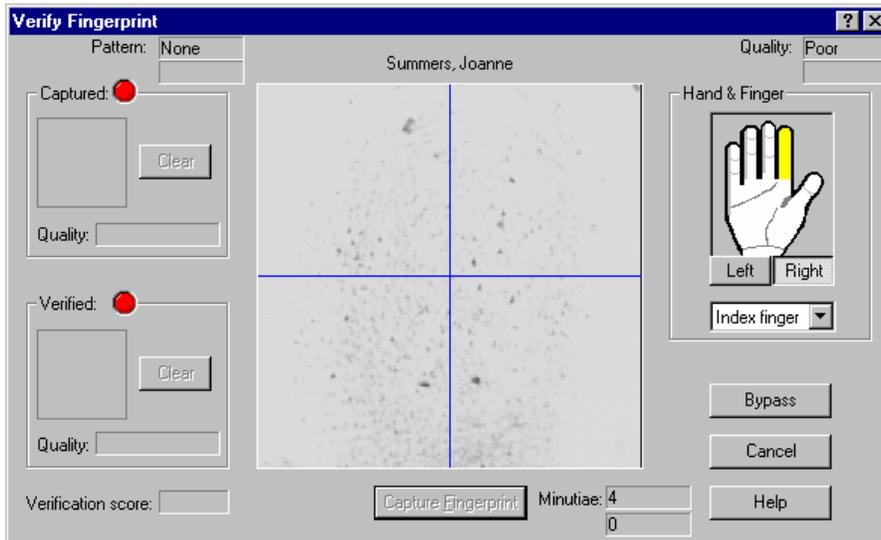
1. When selecting the Create ID Card Navigator, the VO is presented with the **Capture Fingerprint** dialog box. This dialog box allows the VO to capture a new fingerprint or modify the existing one.



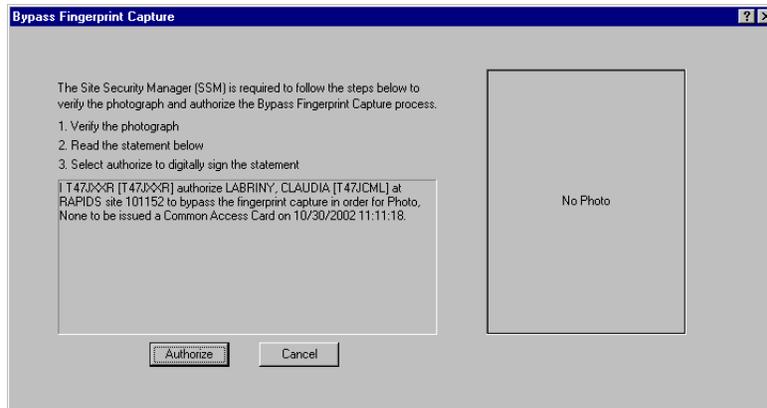
- The VO can bypass this process by three unsuccessful capture/verification attempts. (Click on OK three times).



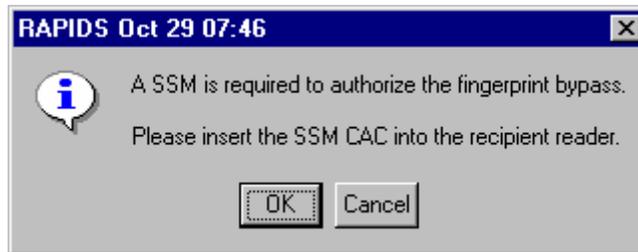
- The OK button is replaced with the Bypass button.



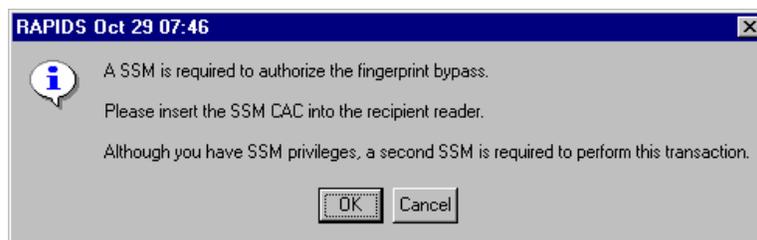
- The Bypass Fingerprint Capture screen appears.



- 5. This screen requires a Site Security Manager (SSM) to use the credentials from his or her CAC to authorize the action of bypassing the fingerprint match.

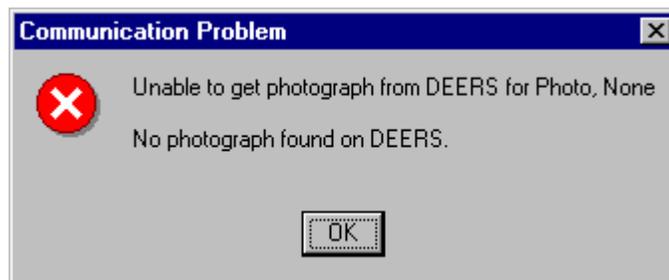


- 6. If the VO initiating the bypass/verification process also serves as SSM for the site, a **second** SSM will be required to authorize the bypass process. RAPIDS prompts the authorizing SSM to enter the CAC into the card recipient reader (which is used normally to read/encode the customer CAC) and enter the PIN associated with the CAC. This process enables the authorizing SSM to skip the fingerprint match/verification process and retrieves the CAC recipient's photograph so that a visual determination can be made.



7. If a photo was previously saved to DEERS, it will display. A photo from DEERS may not be available if the sponsor is being added to DEERS for the first time.

In such cases, the bypass function can be completed by following the instructions for the DD Form 2842 (Department of Defense Public Key Infrastructure Subscriber Certificate of Acceptance and Acknowledgement of Responsibilities). The VO must view a federal government-issued identification credential with a picture, for example *Military ID card* or *Passport*. If a federal government identification credential with a picture is not available, two non-federal government-issued identification cards are required. At least one of the identification cards must show the Subscriber's picture (for example, a drivers license).



8. The statement is digitally signed and the SSM is prompted to remove the CAC from the recipient reader.
9. The VO will be presented with the Capture Photo screen. In both instances, when a photo exists or not, the VO should capture the photo and continue the card issuance process as detailed in *Section 6.3.2* of this training guide.

#### 6.1.10 Create DD Form 1172 Navigator/DSO Scan Information

The  *Create DD Form 1172* Navigator allows the user to update or print a DD Form 1172. Once the family has been saved to DEERS, the user can create the DD Form 1172.

The Create DD Form 1172 Navigator can be accessed using the following procedure.

1. Click the Create Form 1172 icon from the toolbar.  
-or-  
Select **Beneficiary** to select a single family member or **Family** to select multiple family members from the main menu and **Create DD Form 1172** from the drop-down list.
2. The navigator will walk the user through creating and printing the DD Form 1172 for sponsors and/or family members. Select **Finish** when all information is complete.
3. The DD Form 1172 Navigator Summary lists the information that will be included on the DD Form 1172. The summary allows the VO to review the ID card information before it is printed. To make changes to any information listed on the summary page, click **Modify** to page back (in reverse order). Select **Finish** when all information is complete.

- On the Preview DD Form 1172 screen, select **Print** to print the form.

When creating a DD Form 1172, RAPIDS enables default remarks, a default VO, and a default IO. Removing the default check mark next in the check boxes can toggle off these defaults. They can be modified under **Tools|Customize|Navigators|DD Form 1172** on the Workspace window (see *Section 6.11.7* of this training guide).

When the Default Remarks check box is deselected, the user will be prompted to select the remarks that need to appear on the DD Form 1172. The VO can select from the available list of RAPIDS remarks by double clicking on a specific remark. The VO may also enter his/her own remark by typing it in.

When the Default Verifying Official/Issuing Official check boxes are deselected, the user will be prompted to select the appropriate site, and VO, IO, or Temporary VO or IO. When the ID card is to be issued at another facility, the user may deselect printing the IO (in the case of a pre-verified DD Form 1172).

Blank DD Forms 1172 can be printed through the main menu as well as through the DD Form 1172 Navigator. Select **File|Print** from the menu. Options are displayed to print the current view or a blank DD Form 1172. This eliminates the need to use the Create DD Form 1172 Navigator to simply print a blank form.

The Privacy Act Statement can be viewed or printed by selecting **Privacy Act** from the Help option.

**Note:** If a sponsor has two or more personnel categories/conditions to his/her Service Record, or any family member has more than one benefit set period, a user has the ability to select the segment for which he/she would like to print the DD Form 1172. The user would select the appropriate category, relationship, or benefit set from the combo boxes that appear in the diagram below. Grayed text will indicate that the field only has one choice and that the control is read-only. Black text indicates that there is more than one choice and that the field can be changed.

Print DD Form 1172 for:	Relationship		Benefit Set Period	Card Exp. Date
	Type	Condition		
<input type="checkbox"/> Carter, Melissa L.	Spouse	[None]	1982SEP15 - 2002OCT18	2001OCT21 <input checked="" type="checkbox"/>
<input type="checkbox"/> Smith, Jackie	Child	[None]	1997SEP12 - 2001FEB13	2001FEB13 <input checked="" type="checkbox"/>
<input type="checkbox"/> Jules II, Henry	Child	[None]	1997OCT21 - 2001FEB28	2001FEB28 <input checked="" type="checkbox"/>
<input type="checkbox"/> Ward, Bob	Ward	Court Order	1986MAY29 - 2002OCT18	2006NOV27 <input checked="" type="checkbox"/>
<input type="checkbox"/> Jones, James L.	Ward	[None]	1986MAR11 - 2002OCT18	2001OCT21 <input checked="" type="checkbox"/>
<input type="checkbox"/> Smith, Mike	Ward	Court Order	1997MAY29 - 2002OCT18	2006NOV26 <input checked="" type="checkbox"/>
<input type="checkbox"/> Johnson, Brian S.	Child	[None]	1997SEP01 - 2001MAR02	2001MAR02 <input checked="" type="checkbox"/>
<input type="checkbox"/> Hoff, Ghjgh H.	Parent-in-law	[None]	1997JAN07 - 2002OCT18	2001OCT21 <input checked="" type="checkbox"/>
<input type="checkbox"/> Cater, Tim	Parent-in-law	[None]	1997OCT22 - 2002OCT18	2001OCT21 <input checked="" type="checkbox"/>

**RAPIDS Select Relationship Condition Window**

**Note:** To ensure that the DoD has an archive of historical DD Forms 1172 on file, the DSO will

accept paper DD Forms 1172 from ID card facilities for archiving electronically. Only DD Forms 1172 for family members need to be forwarded. Supporting documentation (such as marriage/birth certificate) should not be forwarded to DSO. ID card facilities will no longer be required to file and maintain the paper copies for the life of the card, provided that they are sent to DSO. DSO can reproduce needed DD Forms 1172 upon request by personnel offices or beneficiaries.

DD Forms 1172 must be mailed to DMDC Support Office.

DMDC Support Office  
ATTN: 1172 Scan  
400 Gigling Road  
Seaside, CA 93955-6771

Common Access Card (CAC) recipients must complete the DD Form 2842 (DoD Public Key Infrastructure Subscriber Certificate of Acceptance and Acknowledgement of Responsibilities) prior to receiving their CAC. Recipients who are VOs must complete the DD Form 2841 (DoD PKI Registration Official Certificate of Acceptance and Acknowledgement of Responsibilities) in lieu of the DD Form 2842. DoD Contractors or DoD Civilians not enrolled in DEERS with one of those Personnel Categories must present a completed DD-Form 1172-2 signed by their Personnel Contracting/Civilian Officer.

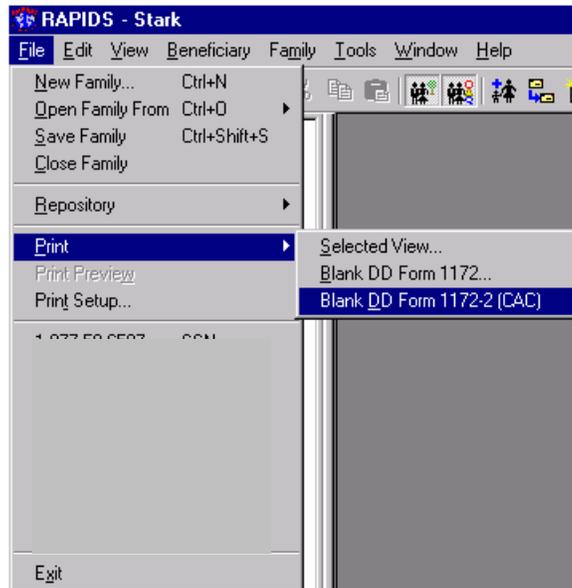
DD Forms 1172-2, DD Forms 2841, and DD Forms 2842 should be packaged and mailed to:

DMDC Support Office  
ATTN: PKI/CAC Scan  
400 Gigling Road  
Seaside, CA 93955-6771

They may be mailed together in the same envelope, but must be separated by paperclip (no staples).

#### **6.1.11 Create DD Form 1172-2**

The 1172-2 is the application for DoD CAC and DEERS enrollment completed and verified by the applicant's designated authority. Officials designated to authorize or verify the 1172-2 are responsible for the form's accuracy. The form is required to add a Personnel Category of DoD Civilian or DoD Contractor to an existing sponsor's record or to enter a new DoD Civilian or DoD Contractor into DEERS. A blank DD Form 1172-2 can be printed through the RAPIDS version 6 application by selecting **File|Print|1172-2** from the menu.




---

## 6.2 RAPIDS Joint Data Model Smart Cards

The two types of sponsor ID cards in use prior to the implementation of the CAC were the teslin ID card and the Joint Data Model (JDM) smart card shown below.



If the RAPIDS CAC workstation is configured for downloading Joint Data Model (JDM) applets, the JDM applets can be installed on either newly issued or previously obtained CACs. This will be known by the appearance of a green check in the upper right side of the post-downloading certificates summary screen. The initial issuance of CACs fielded during the CAC beta test will not support the JDM applets, and if attempts were made to update these CACs, the VO will receive a message stating “JDM applets not supported on this card”. In such a case, the recipient’s CAC would need to be reissued.

Administrative privileges are required to select the “Install JDM applets” option through RAPIDS Configuration. Contact the D/RAC / DRSC-E/ DSO-A for assistance. It will be necessary to reopen RAPIDS after making this configuration change.

## 6.3 Using RAPIDS to Issue the CAC

The VO's Windows log on ID and password are stored on his/her CAC. ActivCard utility has been added to Windows allowing the VO to use the log on ID and password from the VO's CAC to log on to the RAPIDS workstation when the VO's PIN is entered. When the VO's CAC is removed from the reader/encoder, the RAPIDS workstation will lock. Only the VO logged in or someone with administrator privileges can then unlock the workstation. If the workstation is locked, and the VO logged on is unavailable to unlock it, contact the D/RAC / D/RSC-E / DSO-A for temporary administrator permissions to unlock the workstation and log off the VO who locked it. **Never power down a workstation that has been locked. It must be properly shutdown first.**

### 6.3.1 Create Card Navigator

The  *Create Card Navigator* allows the user to create a teslin ID card or CAC. Once the family has been saved to DEERS, the user can create the ID card/CAC. The *Create Card Navigator* can be accessed using the following procedure.

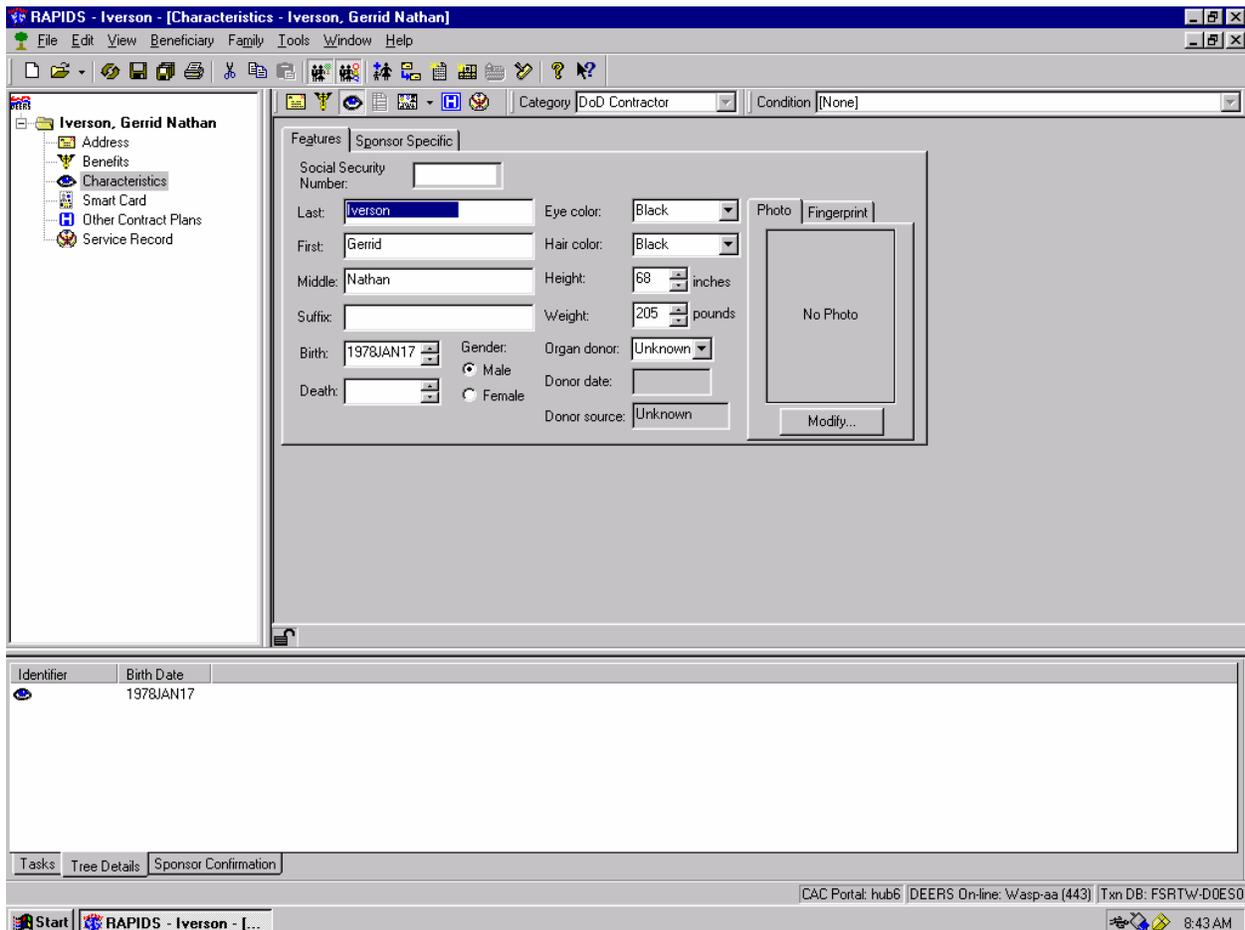
1. From the main menu, select **Beneficiary|ID Card|Create or Family|Create Cards**.  
-or-  
Select the **Create ID Card** icon from the toolbar.
2. Select the specific ID card(s)/CAC(s) to be printed and select **Next** when all information is complete. **Note:** If a sponsor has two or more segments to his/her Service Record or any family member has more than one benefit set period, a user can select the segment for which he/she would like to print the ID card/CAC. Select the appropriate category, relationship, or benefit set. Gray text will indicate that the field only has one choice and that the control is read-only. Black text indicates that there is more than one choice and that the field can be changed.
3. The RAPIDS Capture Fingerprint dialog box may appear for the sponsor. (Refer to *Section 6.1.8* of this training guide).
4. At the Modify Photo screen, adjust the camera using the onscreen buttons. Ensure that the background for the photo is white or off-white. Zoom in or out as needed. Click **Take Photo** to take the photograph when ready. Use the brightness and contrast sliders to adjust the photograph as needed. Click **OK** to continue or retake the picture if necessary.
5. The navigator guides the user to the Create Card Summary that lists all information that will be printed on the ID card/CAC. To make changes to any information listed on the summary page, click **Modify** to page back (in reverse order).
6. Select **Print** to continue. The RAPIDS software will instruct the user through all the necessary steps for printing either the teslin ID card or the CAC.

### 6.3.2 CAC Issuance Process Flow

When creating a CAC, follow the procedures as listed in the AFI 36-3026(I) and steps detailed in this training guide to verify and input all information required during ID card issue. Pay particular attention to ensure that the sponsor’s name displays in RAPIDS exactly as it should be printed on the CAC. Capitalize only the characters that require capitalization (such as the first letter of the name). DEERS allows up to 26 characters for the last name, 20 characters for the first name, 20 for the middle name, and a four-character suffix. The name on the certificate allows a maximum of 64 characters for the common name. As a result, some truncation of names on the certificates may occur.

Ensure that the Work E-mail Address is added correctly to the Service Record. Without the work e-mail address, RAPIDS will not generate the two e-mail certificates. It is important that RAPIDS have the correct e-mail address because this is used to generate the e-mail certificates. If the address on the certificate does not match the address actually being used, the application may reject the certificate.

Organ donor information is now printed on the CAC for military sponsors. The VO should inform Active Duty and Guard/Reserve members what organ donor status is reflected in their RAPIDS record before creating the CAC. The VO may update this information through the sponsor’s *Characteristics* view.



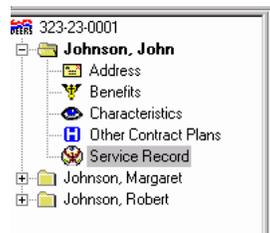
For DoD Civil Service, DoD Contractor, or Foreign National sponsors that are not already entered into DEERS, use the information from the signed and verified DD Form 1172-2 to enter the sponsor into DEERS through the Add Personnel Category Navigator. For the End of Contract/Employment field, the VO should enter the end date as listed on the DD Form 1172-2. For detailed information on adding a Contractor, refer to training scenario *as detailed in Section 7.37* training guide.

Family members need not be added to DoD Civil Service or DoD Contractor records unless eligible for benefits (such as family member with an “Accompanying Sponsor” Relationship Condition) and never without documentation. **Note:** Civilian personnel tapes send the birth month and year for Civilian employees to DEERS. Since the actual birthday is not sent to DEERS, the first of the month may display. VOs should confirm (and update if necessary) the date of birth on all DoD Civilians.

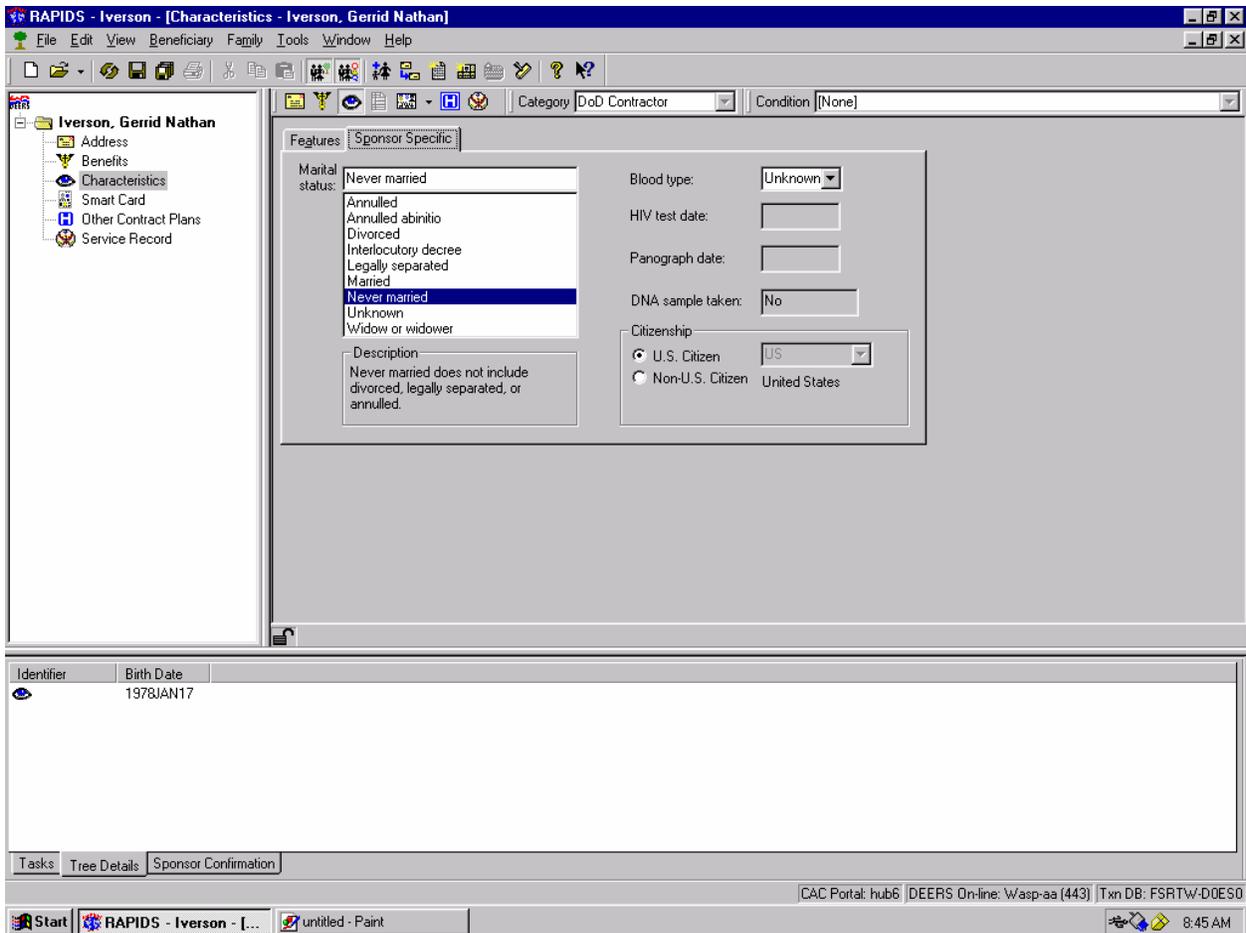
The CAC expiration date will be no more than three years from the issuance date. This is the date that the certificates expire. Military sponsors with end dates in RAPIDS over three years should be assured that the personnel category and entitlements are not expiring.

To create a CAC, use the following procedure:

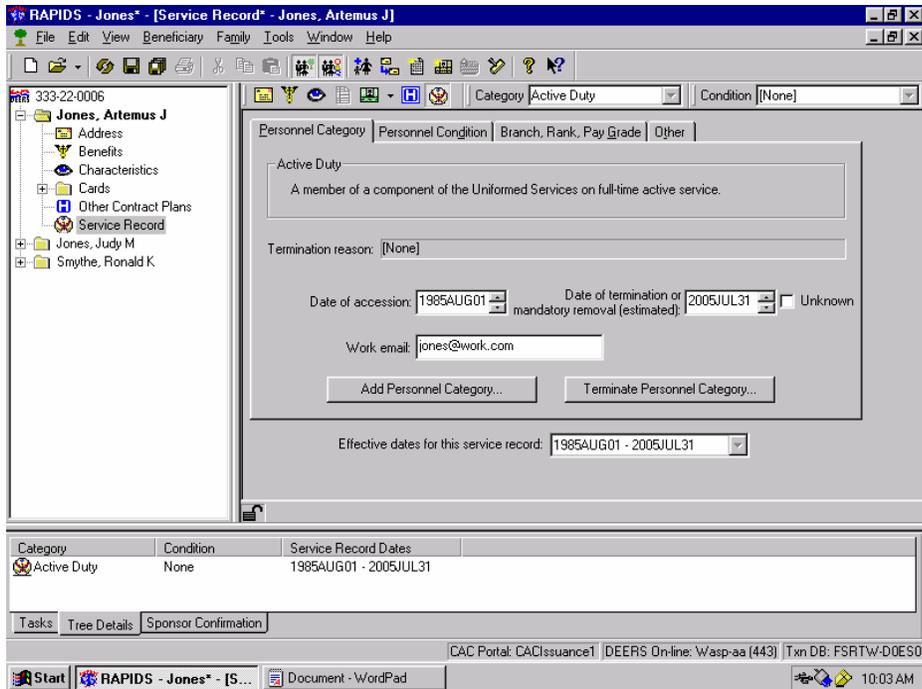
1. Open Family from DEERS.
2. If the Family is new, create a new family from the signed DD Form 1172-2.



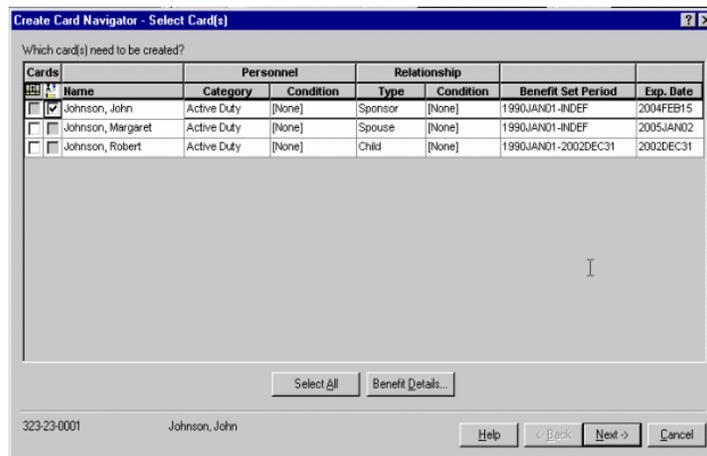
3. Verify/enter all sponsor information. Update Organ Donor status and citizenship information. Citizenship is now a required field that must be verified and selected for new sponsors and verified for existing sponsors. A listing of the countries and country codes can be found in RAPIDS Online Help by searching on Foreign Country code.



**Note:** Do not add family members to DoD Civilians or Contractor personnel. If the member has family members that meet the requirements of accompanying the sponsor overseas, these family members can be added with proper documentation.

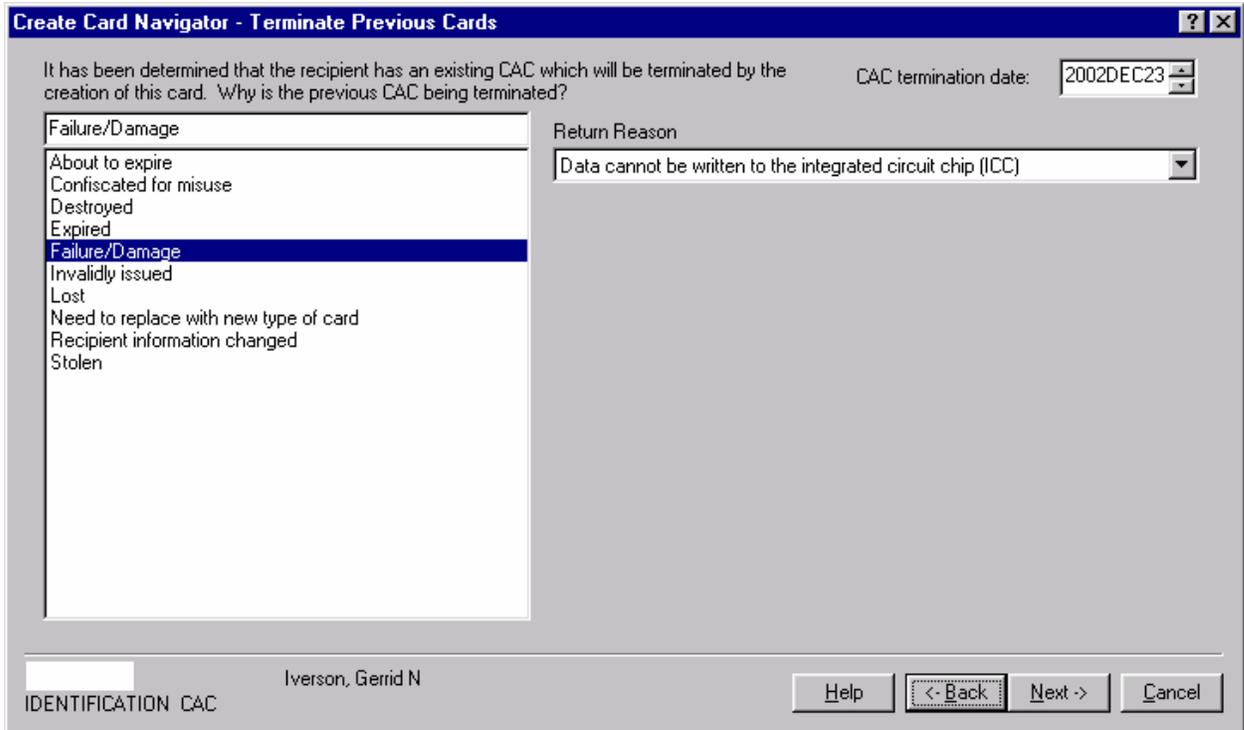


- When opening the Create Card Navigator, the Cards field at the left of the Navigator dialog box contains two icons. Click on the **Create Card Icon** and check the Sponsor's CAC checkbox to the left of the sponsor's name.

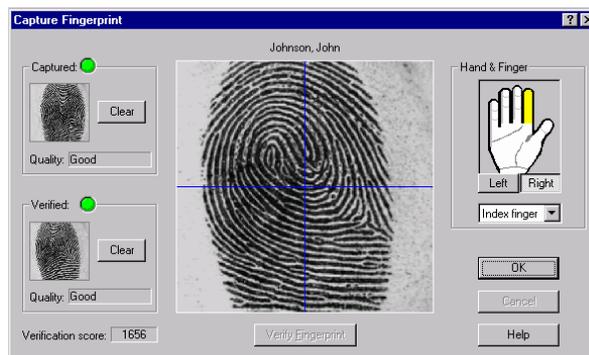


**Note:** Family members and retirees are not authorized to receive the CAC. The CAC icon checkbox will be disabled for anyone other than the sponsor and will be enabled or disabled for the sponsor, depending on the sponsors' eligibility. Click the **Next** button to proceed.

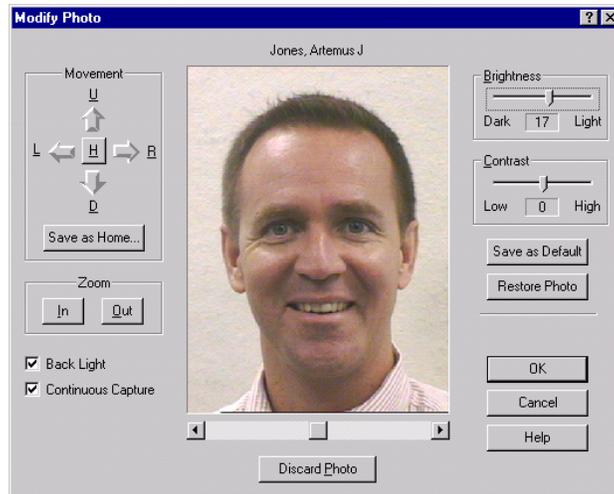
- Select a reason for terminating the previous card from the list.



6. Capture Fingerprint. When issuing a CAC, RAPIDS will prompt the VO to capture the sponsor’s fingerprint. If the sponsor’s DEERS record has a prior fingerprint stored, RAPIDS first verifies that the fingerprint matches the previous one in DEERS. This allows the VO to verify the CAC recipient’s identity. If the fingerprints match, the VO proceeds with issuing the CAC. If no fingerprint is available on DEERS or the fingerprints do not match, the VO can attempt to retake the fingerprint. After three unsuccessful attempts to match the fingerprint, the VO can choose to override or bypass the software if proper documentation verifies the identity of the CAC recipient. All decisions by a VO to override a failed fingerprint match are audited. Refer to *Section 6.1.9* of this training guide for instructions on this navigator.



7. Take Photo.

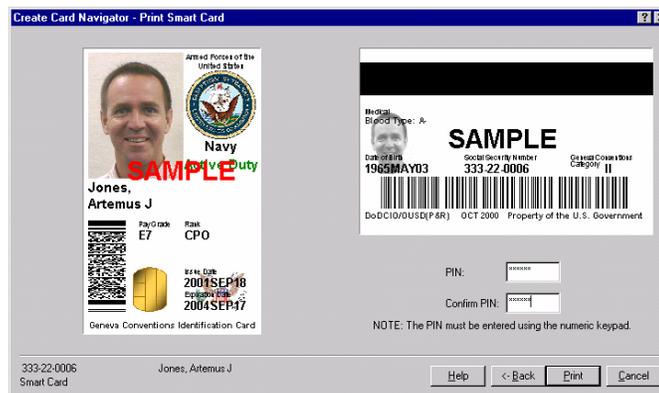


- After taking the card recipient’s photograph, the system will open the Print Card page of the Create Card Navigator. A preview of the CAC appears, as well as the request for the recipient to enter their PIN. Ensure that all of the sponsor’s information is correct and that the sponsor is provided an opportunity to review the information and photo, if so desired.

A vital piece of the Common Access Card (CAC) is the Personal Identification Number (PIN) used to access the information on the chip. The PIN protects information on the chip from unauthorized access to person and personnel data including the CAC recipient’s private keys.

Because of the personal nature of the PIN, the RAPIDS VO should refrain from recommending ideas, prompts, or hints while the customer is creating their PIN. Recommended guidance is: “Please create a six to eight digit numeric PIN. Try to use a number that you can easily remember but something that cannot be easily guessed by others. Do not use a number that is printed on the card.”

The VO should stress the importance of remembering and protecting this number. After three unsuccessful attempts to log in with a PIN, the CAC will become locked. This currently requires the CAC recipient to return to a RAPIDS workstation to unlock the CAC.



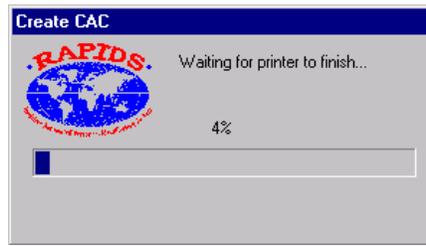
**Note:** This PIN will be used to access personal entitlements, such as commissary and

exchange privileges. This PIN should only be known by the cardholder. The CAC recipient should select and enter his/her private PIN into the system via the numeric PIN pad (preferred) or the keypad on the keyboard. Using the number keys along the top of the keyboard will not work. Ensure that the keypad is adequately shielded from the view of the VO and others.

9. Instruct the card recipient to type the PIN a second time for verification. An error message will inform the sponsor if the PINs entered do not match.



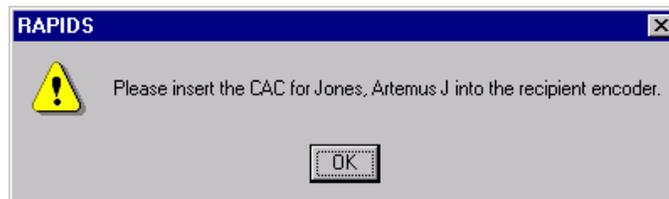
10. Ensure that the printer is ready and the CAC stock is properly loaded in the printer's feeder, and select the **Print** button.



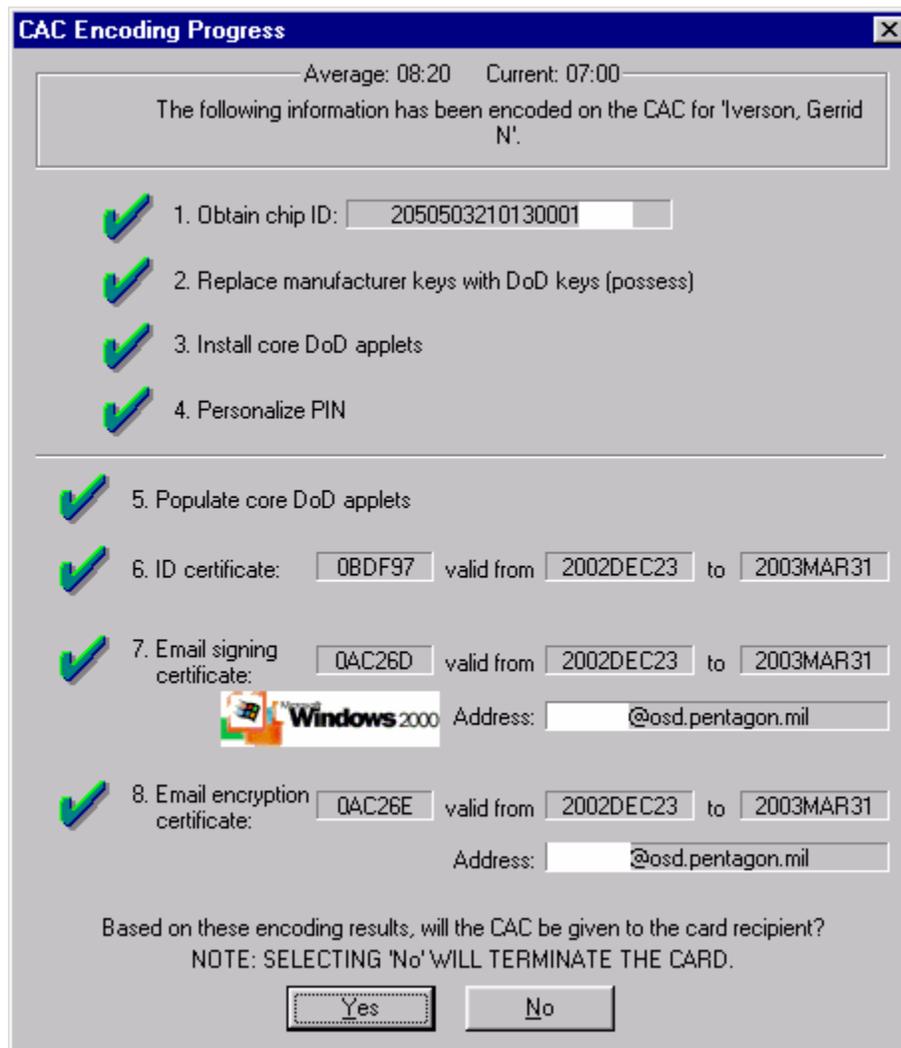
11. After printing, RAPIDS will prompt the VO to verify the Code 39 bar code.



12. Once the bar code has been verified, inspect the front and back of the card. If the CAC did not meet inspection standards, select **No** at the "Did the CAC print properly?" prompt. If the card is deemed of acceptable quality, select **Yes** at the prompt.
13. RAPIDS prompts the VO to insert the card recipient's CAC into the reader/encoder. Insert the CAC into the CAC smart card reader/encoder, chip up and chip first.



14. Encode the CAC. This process may take five or more minutes, depending on the quality of communications available to the site. When the VO inserts the CAC into the smart card reader/encoder, two separate processes are completed. (1) Via a secure SSL session with the Issuance Portal, the ICC is encoded with personal data and associated applet. (2) Via a secure SSL session with the CA and Issuance Portal, the three certificates (identity, digital signature, and e-mail encryption) are created, issued, and encoded on the ICC with the associated applet. The encoding progress dialog reflects the processes as they run, keeping the VO aware of the progression of the encoding process. The dialog also keeps track of average successful encoding times and displays the current encoding time. These transactions must be saved successfully for the CAC issuance process to be complete. Pay attention to the message boxes, as any error messages must be recorded and will dictate further steps to complete the CAC encoding. After the CAC is encoded, RAPIDS saves the transactions to DEERS.
15. Upon completion of encoding, RAPIDS will check the certificates that have been loaded onto the CAC's ICC.



16. If the CAC recipient is also a VO, additional steps are required to add VO privileges. These steps are detailed in *Section 9.2* of this training guide.

After the card is printed and encoded, RAPIDS prompts the VO to remove the card from the reader. RAPIDS then saves the photograph, the CAC, and fingerprint transactions to DEERS.

Policy directed from the Office of the Secretary of Defense (OSD) prohibits amending, modifying, or overprinting on the Common Access Card (CAC). The policy specifically states that no holes shall be punched into the CAC. Also, no stickers or other adhesive materials are to be placed on either side of the CAC.

Please inform each CAC recipient of this requirement before issuing the card. Verifying Officials should briefly mention the policy to the recipient while the card is encoding. A simple statement such as “No stickers or hole punching permitted.” will suffice.

To view the official policy memorandum visit the VO web site. Go to [https://www.dmdc.osd.mil/vois/docs/policy\\_instruction/CACpolicy.pdf](https://www.dmdc.osd.mil/vois/docs/policy_instruction/CACpolicy.pdf) to read CAC Policy Memo 1-16-2001. The referenced requirement can be found on page four of the memorandum under Restrictio

### 6.3.3 CAC Description

#### 6.3.3.1 Front of the CAC



*Unauthorized reproduction, imitation, or likeness of the CAC is punishable under 18 U.S.C Section 701.*

*Front of CAC*

**The front of the CAC contains:**

- Organization Seal.
- Branch of Service.

- Color Photograph of the card recipient.
- Personnel Category/Reason for Affiliation.
- Name.
- Rank and Pay Grade/Grade- if applicable for the card type.
- Issue Date – This represents the date at which the card is considered valid.
- Expiration Date – This date is the earlier of either three years or the individual’s end of eligibility to DoD benefits.
- PDF417 Bar Code - 2-dimensional bar code that contains most of the textual data from the CAC, the new DoD EDIPI, and SSN.
- Card Type/Title - such as, Armed Forces of the United States, United States DoD/Uniformed Services, etc.
- Card Identification Information - such as, Geneva Conventions Identification Card, Identification and Privilege Card, etc.
- Optically Variable Device for enhanced security (Hologram).
- ICC - contains the smart card operating system, special smart card applications (called applets), private PIN, up to three PKI certificates (identity, digital signature, and e-mail encryption) and their associated private keys, and most of the textual data from the CAC. The information stored on the chip includes:

Blood Type	First, Middle, and Last Name
Branch of Service	Gender
Card Expiration Date	Government Agency
Card Issue Date	Meal Entitlement Code
Card Security Code	Medical Benefits End Date
Citizenship	Name Suffix
Civilian Health Care Entitlement Type Code	Non-Government Agency
Date of Birth	Non-medical Benefits End Calendar Date
Demographic Date Chip Expiration Date	Organ Donor
Direct Care Benefit Type Code	Pay Category
DoD Contractor Function Code	Pay Grade
DoD EDIPI	PKI Functionality
Duty Status	Rank
Entitlement Condition	User PIN
Exchange, Commissary, and Morale, Welfare, and Recreation (MWR) Codes	

### 6.3.3.2 Back of the CAC



*Unauthorized reproduction, imitation, or likeness of the CAC is punishable under 18 U.S.C. Section 701.*

#### *Back of CAC*

#### **The back of the CAC contains:**

- Medical Information and Benefits block.
- Magnetic Stripe - standard three-track magnetic stripe.
- Code 39 Bar Code - contains some of the textual data from the CAC, the new DoD EDIPI, and SSN.
- Date of Birth.
- SSN (or other Person Identifier).
- Geneva Conventions Category.
- Blood Type.
- Organ Donor Status – The possible values are Yes, No, and Undecided. Card recipients that have not yet indicated they are willing to be an organ donor will have no designation printed on the card.
- Footer - DoDCIO/OU8D (P&R), effective date of card format, and Property of United States Government.

If, due to multiple personnel categories, a person requires multiple CACs, all CACs are to receive the identity certificates. The e-mail certificate will be requested if the e-mail address is present in the Service Record view. For dual eligibility situations (such as DoD Contractor and Reservist), both eligible CACs will be given identity certificates. E-mail certificates will be added to the CAC if the corresponding personnel category has an e-mail certificate.

### 6.3.4 Certificate Revocation

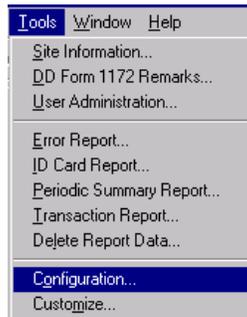
When a card is being terminated, RAPIDS will revoke the certificates associated with the CAC. RAPIDS will automatically terminate the identity and digital signature certificates for reasons such as a lost card or invalid entry. When a user's e-mail address is changed, the old e-mail certificates will be revoked, and new ones will be issued and placed on the existing CAC. If

information on the card changed or the card has a defective chip, the VO must handle the CAC according to the procedures for card return.

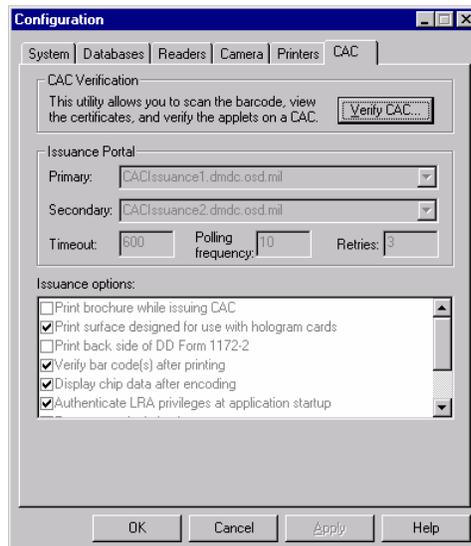
### 6.3.5 Verifying CAC Certificates

The VO can verify each CAC issued for certificates and inform each CAC recipient of the certificates encoded on his/her CAC. This is done automatically by RAPIDS after the CAC's ICC has been encoded, but can also be checked by following these steps.

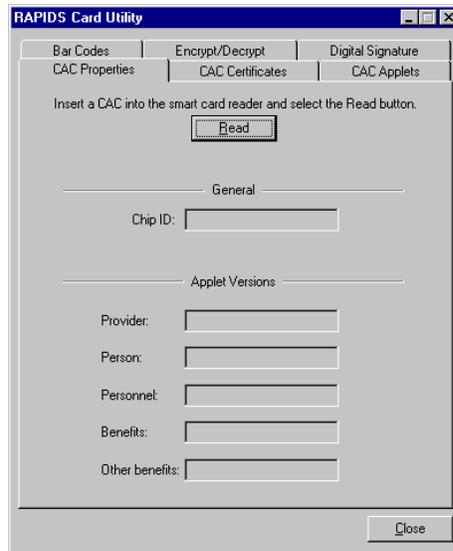
1. Insert the CAC in the CAC smart card reader/encoder. Select **Configuration** from the Tools menu.



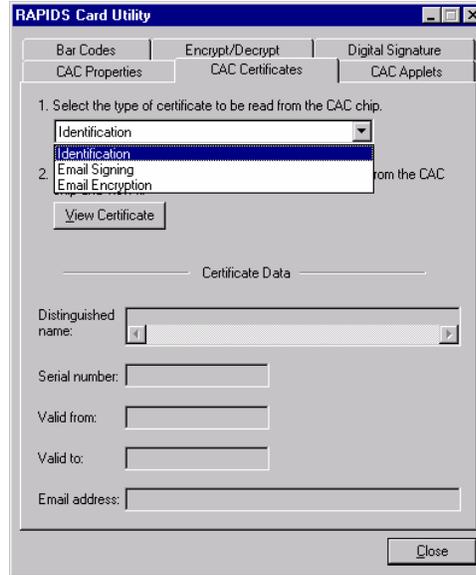
2. Select the **CAC** tab and click the **Verify CAC** button. Next, check to see if any certificates were encoded on the chip by selecting the **CAC Certificates** tab. Verify each certificate separately by highlighting a certificate and select **View Certificate**. The configuration screen refers to the certificates as E-mail Encryption, E-mail Signing, and Identification. This step will help to determine if any certificates were successfully written to the chip.



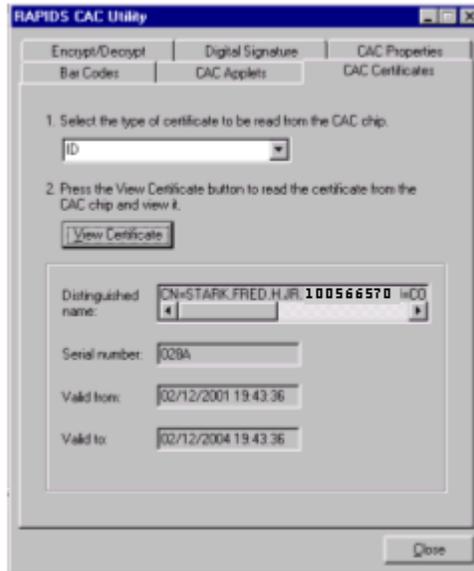
3. Select the **CAC Properties** tab and click on the **Read** button to check for CAC load.



- The **Bar Codes** tab allows the VO to scan either the Code 39 or PDF417 bar code.
  - The **CAC Applets** tab allows the VO to read benefits, person, or personnel information from the CAC chip when inserted into the reader.
  - The **CAC Certificates** tab allows the VO to read the E-mail Encipherment, E-mail Signing, or ID Certificate from the CAC chip when inserted into the reader.
  - The **Digital Signature** tab allows the VO to create a digital signature.
  - The **CAC Properties** tab allows the VO to read the chip ID, provider version, benefits version, other benefits version, person version, and personnel version from the CAC.
  - The **Encrypt/Decrypt** tab allows the VO to encrypt or decrypt a string of text.
4. Select the **CAC Certificates** tab. Using the drop-down menu, select one of the three certificates and click on the **Verify** button. Repeat this process for each of the certificates listed.



**Note:** Each certificate will populate the Verify CAC fields with a Distinguished Name, Serial Number, and Validation Dates.

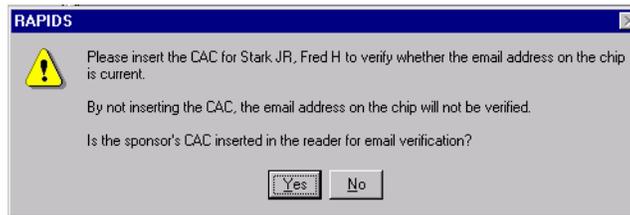


### 6.3.6 Updating a CAC

The procedures listed here can be used to update the E-mail Encryption and E-mail Digital Signature certificates on a CAC. This function will not update the Identity certificate. To update the identity certificate, a new CAC must be issued.

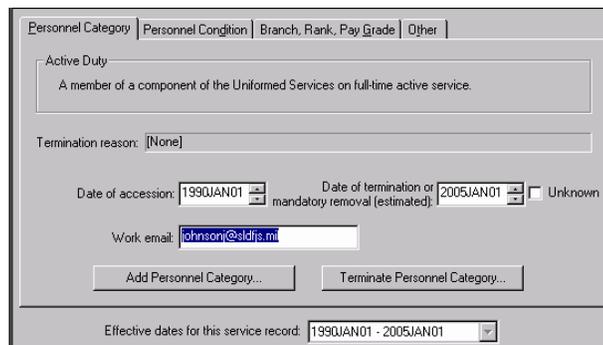
The primary method for updating a CAC is to allow RAPIDS to read the CAC ICC at the time

that the sponsor's record is opened.

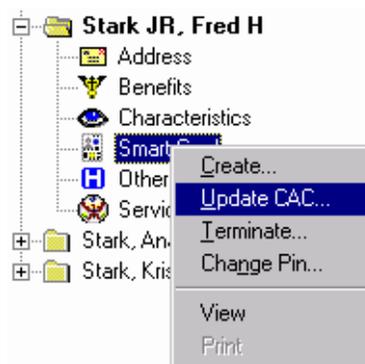


From this point, the following steps can be used to update the e-mail certificates on a CAC:

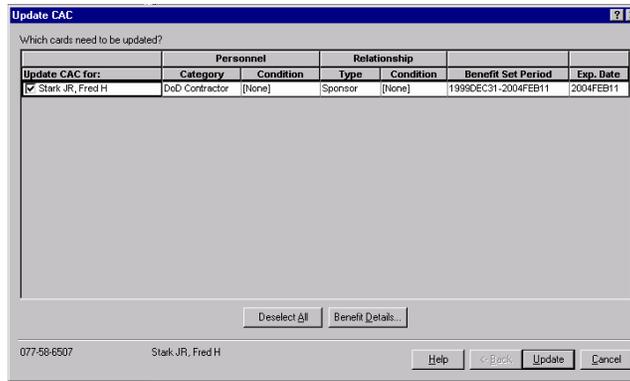
1. Open the sponsor's Service Record and modify the Work E-mail Address from the *Personnel Category* tab.



2. In the RAPIDS Family Tree, right-click on the **CAC** icon and select **Update CAC...** or select the **Update Card** icon from the Tool Bar. The **Update CAC** icon will only display in the Tool Bar if the CAC is highlighted in the Family Tree.



3. Select the card to be updated. The progress meter will display as the chip is updated. This process can also be used to restore a CAC that was not completely encoded due to communication errors.

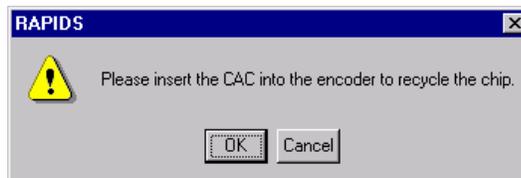


Ensure that the CAC is properly inserted into the reader. Click on the **OK** button to begin the Update process. A progress monitor will display during the update.

### 6.3.7 Recycling a CAC

Recycling a CAC is an administrative function performed by an SSM only. Recycling is not to be used in lieu of updating a CAC or instead of replacing a CAC. To recycle a CAC, erasing any sponsor information stored on the CAC, select the Recycle Chip option under **Tools|CAC Operations** and follow the steps as listed.

1. Insert the CAC to be recycled into the reader/encoder.



2. Click OK. A progress monitor will appear while the CAC is being recycled.

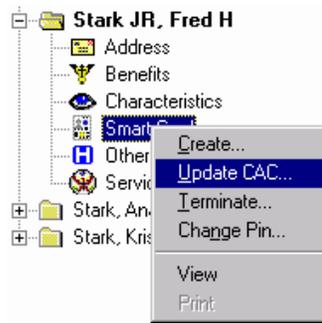



---

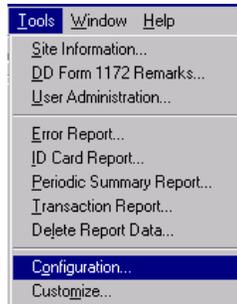
## 6.4 Troubleshooting for a CAC that Errors during Encoding

Each and every CAC must be accounted for. When a card fails during encoding, the VO must complete the following steps to (1) ensure the site does not assume the chip is bad and discard a valid card and (2) ensure consistent troubleshooting procedures for all sites. Use the RAPIDS navigator to print and encode the CAC.

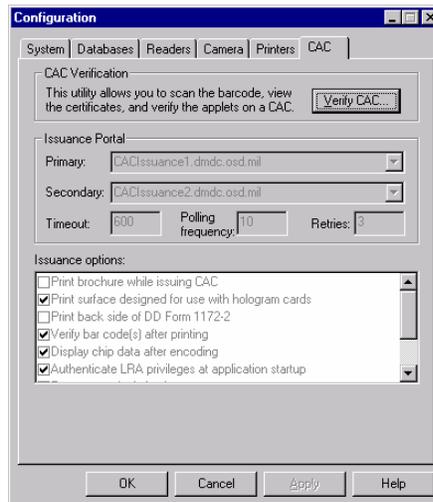
1. Use the “Update CAC” process (Select **Beneficiary|Card|Update CAC**) to reattempt encoding. Using the “Update” command is important because it does not remove data already written to the chip.



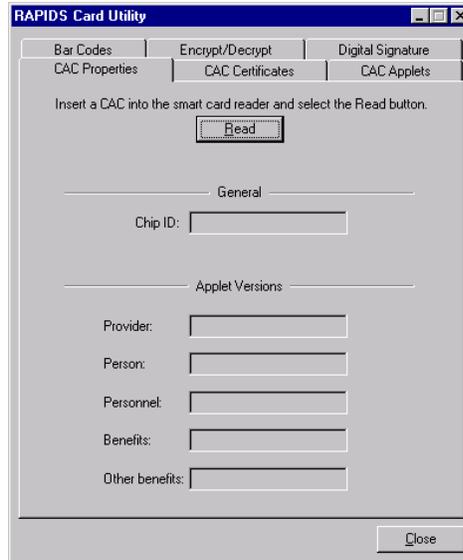
2. If updating fails, cancel out of the Navigator and open **Tools|Configuration**.



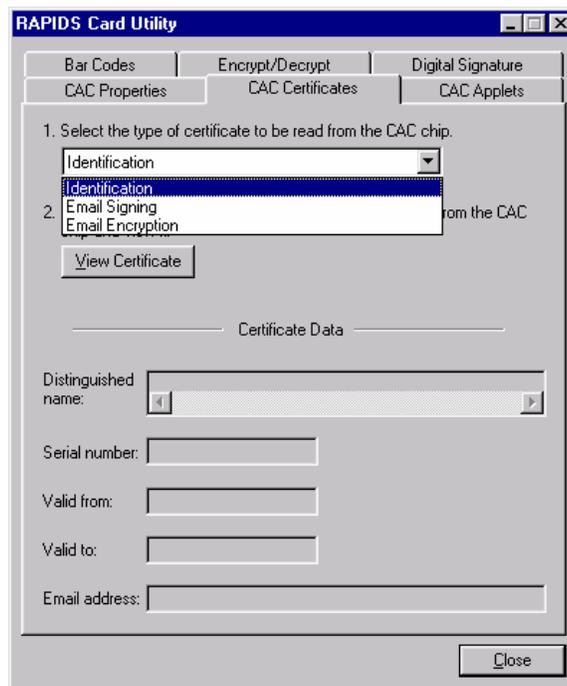
3. Select the **CAC** tab. Select the **Verify CAC** button.



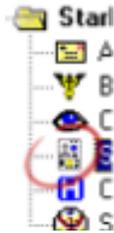
4. Attempt to read the chip by selecting the **CAC Properties** tab. If the CAC properties are displayed, then the problem is not likely to be a malfunctioning chip.



- Next check to see if any certificates were encoded on the chip by selecting the “CAC Certificates” tab. Verify each certificate separately (E-mail Encryption, E-mail Signing, and Identification) by highlighting a certificate and selecting **View Certificate**. This will help to determine if any certificates were successfully written to the chip.



If it is determined that the chip is not at fault, contact the D/RAC, the DRSC-E, or the DSO-A, as applicable, for further assistance in troubleshooting the problem. If communications is at fault (not the chip) reopen the sponsor’s record from DEERS to verify that the CAC was saved to DEERS. If it appears in the ID card view, the card recipient can leave with the CAC to be encoded at a later time.



If the CAC icon is visible in the family tree, then the CAC production was saved to DEERS.

If it is determined that the chip is faulty and it still cannot be encoded after the above attempts, then try a new card.

If a question of whether the CAC was saved to DEERS exists, reopen the sponsor record from DEERS to see if the CAC displays in the Family Tree. If the CAC does display on DEERS, the VO can select the Update function to update the chip.

### 6.4.1 CAC Termination Procedures

When a CAC (or teslin card) needs to be terminated, the process varies based on whether (1) the personnel category/relationship also needs to be terminated (Example: the sponsor retires) or (2) the card itself needs to be terminated so another card can be issued. (Example: the card has been lost.) This action automatically terminates the associated card. To terminate a card without issuing a new card, highlight and right-click on the card requiring termination to bring up the option to **Terminate the Card**. Select the date and reason for termination.

**Create Card Navigator - Terminate Previous Cards**

It has been determined that the recipient has an existing CAC which will be terminated by the creation of this card. Why is the previous CAC being terminated? CAC termination date: 2002DEC23

Failure/Damage  
 About to expire  
 Confiscated for misuse  
 Destroyed  
 Expired  
**Failure/Damage**  
 Invalidly issued  
 Lost  
 Need to replace with new type of card  
 Recipient information changed  
 Stolen

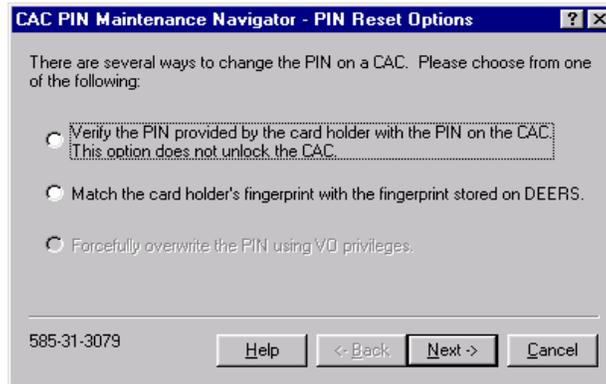
Return Reason  
 Data cannot be written to the integrated circuit chip (ICC)

579-82-7212 Iverson, Gerrid N  
 IDENTIFICATION CAC

Help <- Back Next -> Cancel

## 6.5 PIN Maintenance

When unlocking or changing the PIN of a cardholder, the individual must either provide the current PIN or establish proof of ownership. To access the *PIN Maintenance Navigator*, highlight the CAC that requires a PIN change or select **Beneficiary|ID Card|Change PIN**. The Change PIN dialog is displayed.



RAPIDS provides three PIN reset options:

1. Verify the PIN provided by the card recipient against the PIN on the CAC. Insert the card recipient's CAC into the card recipient reader/encoder. The card recipient must type the old PIN and type a new PIN two times for confirmation. PINs must be entered using the PIN pad.
2. Match the cardholder's fingerprint with the fingerprint stored on DEERS. The Verify Fingerprint dialog box will appear. Capture the cardholder's fingerprint for verification against the fingerprint stored on DEERS. If verification is successful, the cardholder may then enter and re-enter a new PIN.
3. Forcefully overwrite the PIN using VO privileges. The cardholder must enter the new PIN twice. This option is reserved for use as a last resort and only used when the VO can validate the cardholder's identification with verifiable source documents.

**Note:** All PIN maintenance transactions are audited.

---

## 6.6 Online Processing

Online processing is achieved when the communications interface between RAPIDS and DEERS is active. To issue a CAC with a PIN and certificates/keys, communication is necessary among DEERS, the Issuance Portal, and the CA. Online processing is used to perform the following additional functions:

1. Open and update records from the DEERS database.
2. Add new families to DEERS.
3. Save information to the DEERS database.

4. Change DEERS password.

Throughout this Training Guide (unless offline is specified), all instruction refers to online processing.

---

## **6.7 Offline Processing**

Prior to CAC, offline processing occurred only when the communications interface between RAPIDS and DEERS is inactive and the user is not able to open information from or send family data to the DEERS database. An application and ID card can be created, but the data on the ID card may not reflect the data in the DEERS database. Depending on the VO's selection, RAPIDS will either attempt to return to online mode or allow the user to add the family in offline mode. Users should add only the segment for which the DD Form 1172 or ID card is being produced. Example: If an Active Duty sponsor is retiring, the user should enter retirement category information only. When RAPIDS comes back online, the Active Duty record in DEERS will be updated to reflect the retirement category. After completing the transaction the user must attempt to save the family record. Records created in offline mode are always saved offline. RAPIDS edits are enforced in offline mode in exactly the same fashion as they are enforced in online mode.

When in offline mode, the notification area of the RAPIDS application (lower right hand corner) will display the status as "Offline." Users will need to input family data manually if they require a DD Form 1172 or ID card. Offline records are stored on the server, and an attempt is automatically made to transmit the offline records every 30 minutes. In addition, users can manually double-click the word "Offline" and RAPIDS will attempt to reestablish connection to the DEERS database. An explanation is provided if the process to reestablish communication fails. Processing of offline records is an unattended process. It is not necessary for each VO to manually transmit each offline record. A user cannot inhibit a record from being automatically transmitted to DEERS after communication is restored.

The following restrictions apply for producing offline ID cards.

1. RAPIDS will not run, and an ID card cannot be issued if offline records cannot be stored on the RAPIDS server, i.e., the workstation is disconnected from the server. To process offline, it is necessary for the workstations to communicate with the RAPIDS server.
2. With RAPIDS processing in an offline mode, the offline data cannot be saved to DEERS until communication with DEERS is restored. Offline sites do not have the capability to add TINs and FINs.

### **6.7.1 Offline Modes for CAC Production**

Before a VO can begin to issue a CAC, RAPIDS must confirm:

1. The VO has entered the correct PIN.
2. The VO has selected the correct certificate from the dialog box and communication with

the issuance portal has been established.

3. The VO's fingerprint has been verified.
4. The RAPIDS workstation has established communication with DEERS when the family was last opened.

If any of these criteria do not exist, a CAC cannot be printed and encoded. With CAC, the definition for offline processing has expanded because communication between three separate external servers (and communication with the RAPIDS server) is required to complete the CAC issuance. Different modes of offline now exist: (1) Offline to the DEERS database, (2) Offline to the Issuance Portal/Hub, and (3) Offline to the CA. The extent of CAC production completion depends on which communications link is down or unavailable. The RAPIDS application error messages will assist the VO in determining the type of card that can be issued. The following paragraphs describe the offline modes of operation for CAC production.

“Offline to DEERS” refers to the unavailability of communication with the DEERS database. As with prior versions of RAPIDS and for teslin ID card production, operating in offline mode is encouraged. The card recipient's fingerprint cannot be verified against his/her DEERS record and the EDIPI cannot be generated. A temporary CAC without an ICC is all that can be issued. The card will be used strictly for identification purposes. An EDIPI of zero will be generated in the bar codes, and the expiration date for the card will be within 280 days. The time scale is contingent upon whether or not the card recipient is deployed. The card recipient will need to return when communication with DEERS has been reestablished to receive his/her CAC before the temporary card expires.

“Offline to Hub” refers to the unavailability of communication with the Issuance Portal/Hub. The EDIPI can be generated and saved in DEERS. A temporary CAC without an ICC is all that can be issued. The card will be used strictly for identification purposes. The card recipient will need to return when communication with the ActivCard Issuance Portal/HUB has been reestablished, in order to have his/her CAC issued and encoded with the Demographics applet, certificates, and PIN.

“Offline to CA” refers to the unavailability of communication with the CA. A temporary CAC without an ICC is all that can be issued. The card will be used strictly for identification purposes. The card recipient will need to return when communication with the CA has been reestablished, in order to have his/her CAC encoded with the certificates.

The use of chipless (non- ICC) plastic cardstock is not authorized unless communication with DEERS, the Issuance Portal (IP), or the CA is unavailable. RAPIDS will prompt the VO to use chipless cardstock when appropriate. At all other times, utilize normal CAC cardstock. Use of chipless cardstock when not prompted is not authorized and will cause your site to reflect high encoding failure rates. Issuing a chipless card will terminate a sponsor's previously issued card.

The chipless card is a legitimate form of identification and is valid for no more than 280 days. During this time, however, the recipient of the chipless card will be unable to access the Public Key Infrastructure (PKI). The need to access the PKI is widespread and quickly growing. Because of this, it is important that all recipients of a chipless card return after communications

have been reestablished. They will then need to receive a new CAC with the required PKI certificates encoded onto the chip. If you have questions as to when to use chipless cards, call the DEERS/RAPIDS Assistance Center and ask to speak to a Field Service Representative.

Note: If the sponsor's teslin card is still valid, return the sponsor's teslin card and have the sponsor return to receive his/her CAC when communication has been reestablished.

---

## **6.8 Smart Card Handling and Storage**

Plastic cardstock must be kept clean. Any dust or debris on the cards affects the overall appearance of the printed card and can cause extensive damage to the print head. Any fingerprints on the top or bottom surface of the cardstock affect the printing, as well as the bond between the laminate and the cardstock. The most common failure in plastic card printers is damage to the print head, and it is an expensive item to replace. To keep from damaging the print head and to ensure the best quality printing and lamination for the CAC, follow the recommendations listed below.

1. If the plastic smart cardstock is dropped on the floor, it should not be passed through the card printer. The cost of replacing a print head far exceeds the cost of discarding a few cards. Any scratches on the card may be magnified once the card has been produced. Discard any cards with surface scratches.
2. Cards should be stored in their original shipping trays/boxes to ensure that the cards are free of dust and dirt. As the cards are removed for printing, keep plastic wrap around the cards until they are ready for production.
3. The best precaution is to minimize handling of the cards. The less the cards are handled, the greater the opportunity of high-quality card production. When loading cards into the printer, only touch them at their edges, and add them as a single stack. Cards should not come in frequent contact with hands; natural oils on the hands can be transferred to the cards and cause photo degradation and smearing of printing or colors.
4. Rubber bands should not touch the surface of the cards. Rubber bands are typically petroleum based and can transfer a substance on the card, causing a void in the printed card.
5. Avoid rubbing cards together to prevent scratching the card surfaces, which will cause voids in the printed card.
6. Cards can be affected by heat or humidity and should be stored at room temperature.

Always load cards into the printer's card input tray with the ICC/chip facing up and the magnetic stripe facing down and towards the rear of the printer. The printer's card input tray is capable of holding up to 100 cards. CAC cardstock should not be removed from the printer. Excessive handling of the CAC cardstock (such as removing it from the printer on a regular basis) is not recommended, as this will degrade the print quality.

## 6.9 CAC Consumables

RAPIDS sites continue to be responsible for teslin cardstock and plain white 8 1/2" X 11" paper for the laser printer. Sites should continue to procure the necessary teslin cardstock from their normal Service channels.

D/R Ops Div/DMDC will provide RAPIDS sites with CAC cardstock based on their ID card production volume. Cardstock with and without chips will be provided. An initial supply of CAC cardstock will be provided when the CAC-production hardware and software are installed at a site. The automated card management system will be used to handle all CAC stock and consumable handling and ordering.

Whenever CAC cardstock is received, it should be kept in the shrink-wrapped package until it is loaded into the Fargo ProL plastic card printer. CAC cardstock within the Fargo printer should not be removed from the printer when not in use (i.e. overnight). When loading the printer with cardstock, be sure to handle the cardstock by the edges only. Any fingerprints, dirt, or dust on the face (top or bottom) of the cardstock will cause print quality degradation and will increase the probability of jams and cause damage to the printhead within the printer.

Sites are responsible for safeguarding their CAC and teslin card stock. The term “safeguarding” is a loose term, open to interpretation by the site. Cardstock is not a controlled substance and does not have to be kept in a safe. A locked office or desk drawer inside a locked facility may be considered safeguarding.

### 6.9.1 Printer Ribbons, Laminate, and Toner Cartridges

D/R Ops Div/DMDC will provide RAPIDS sites with color printer ribbons and laminate rolls based on their ID card production volume and to match the quantity of cardstock provided to the site. The roll of laminate used within the printer should be used within 12 months after receipt from the manufacturer. One smart card printer ribbon will print approximately 250 cards and should be used within 12 months after receipt from the manufacturer. Smart card printer ribbons require protection from excessive heat, humidity, dust, and light. One cleaning kit provides 50 cleaning cards for every 250 cards printed. The cleaning card used to clean the card feed assembly can also be used to clean the rollers.

RAPIDS sites continue to be responsible for providing toner cartridges for the laser printer. In addition, the RAPIDS site is responsible for monitoring the use of consumables such as cardstock, cleaning kits, and ribbons.

Whenever CAC color printer ribbons and laminate rolls are received, these should be kept in the shrink-wrapped package until loaded into the Fargo ProL plastic card printer. It is also important to store them in a cool and dry place, because heat and humidity degrade these products. Additionally, they have a shelf life of only 12-18 months.

Sites are responsible for removing any printer ribbons/laminate rolls/cardstock or toner cartridges from the D/R Ops Div provided printers prior to sending the printers in for repair. Ensure that the fingerprint scanner’s dongle is detached from the printer cable and kept at the

site. It should not be returned with the printer for repair.

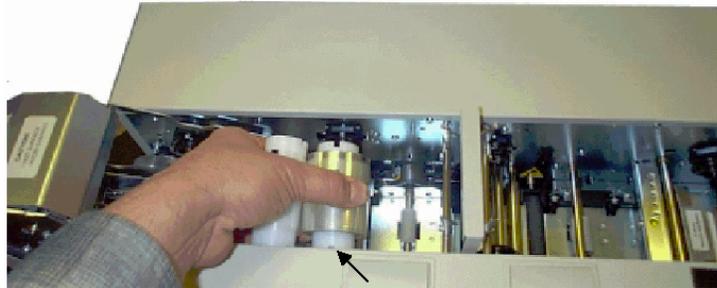
Each cleaning kit contains:

- 50 cleaning cards.
- 50 cleaning pads.
- Four cleaning pens.

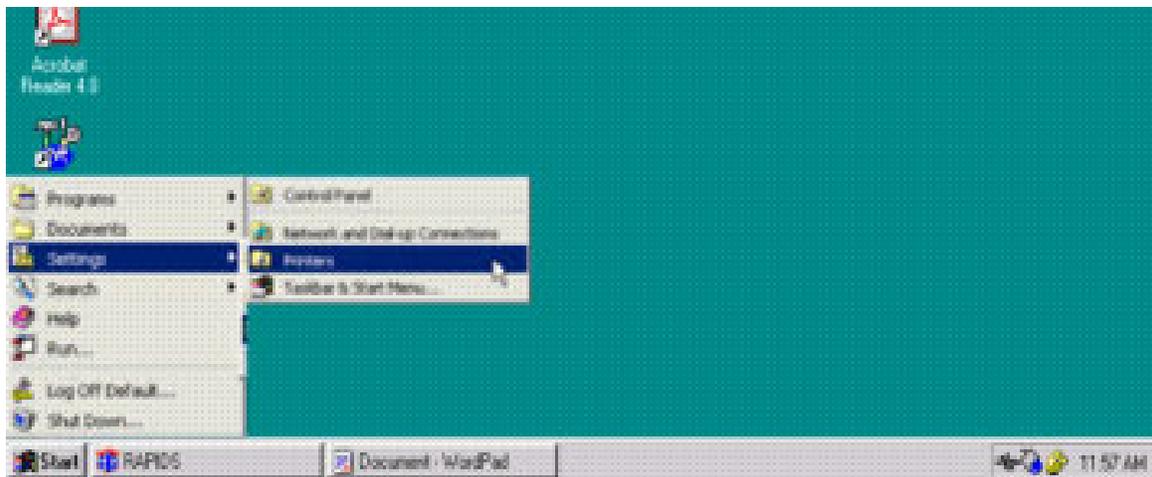
### **6.9.2 Fargo ProL Printer Calibration Procedure**

After cleaning the printer, changing each laminate roll, printer ribbon, or after physically moving the Fargo ProL printer, the VO must recalibrate the printer to ensure consistent printer operation. To calibrate the Fargo ProL printer the VO may refer to the Fargo ProL printer manual or follow the instructions below:

1. Remove the color ribbon and laminate from the printer and close the printer covers.



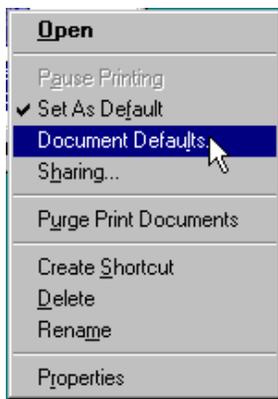
2. Click on **Start|Settings|Printers**.



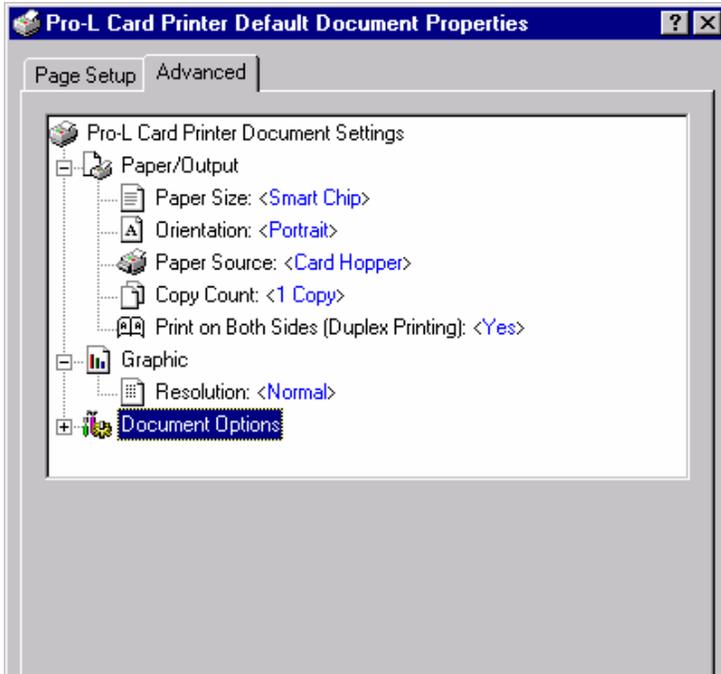
3. Right-click on ProL Color ID Printer.



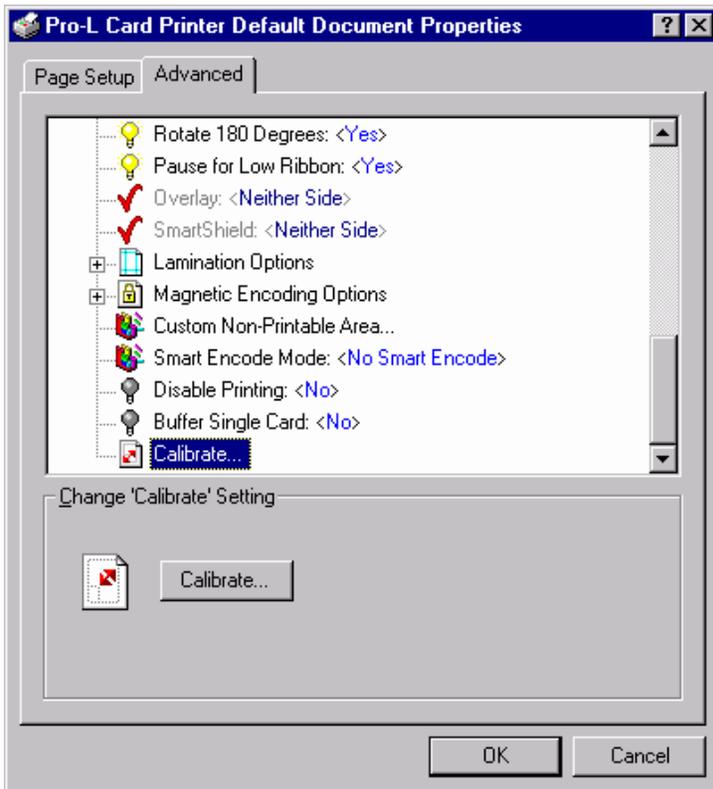
4. Select **Document Defaults**.



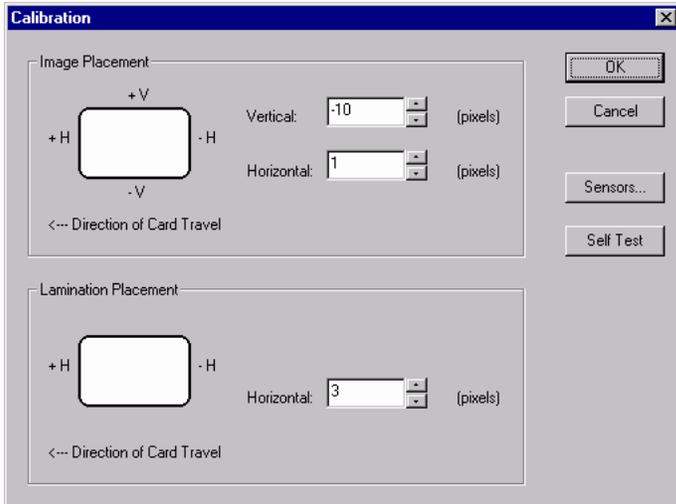
5. Click on the **Advanced** tab, open the **Document Options** section and highlight **Printer Calibration Options**.



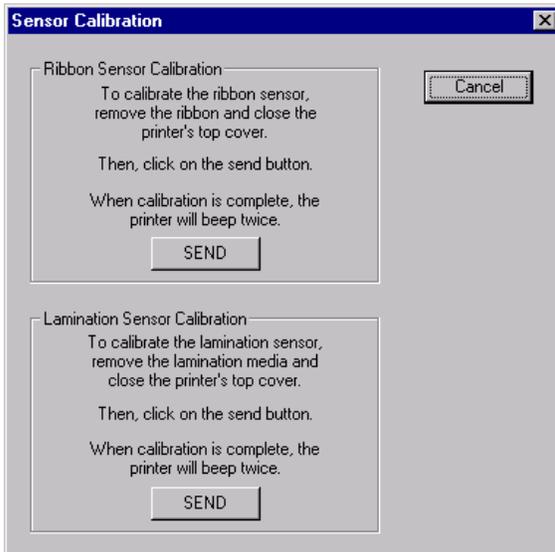
6. Click on the **Calibrate...** button.



7. Click on the **Sensors** button.



8. Ensure that the ribbon or laminate are removed and close the printer's top covers. Click on the **Send** button depending on the calibration task.



9. The printer will beep twice when the calibration is done.
10. Click on the **Cancel** button and then the **OK** button.
11. Install the ribbon laminate and CAC stock in the printer.

As the printer ribbon has an image of each Military sponsor's SSN, you must contact your local Security Department for guidance/policy/procedures for used printer ribbon destruction/disposal. The Fargo printer ribbons and cores should not be burned as the polystyrene and/or PVC cores will emit fluorocarbon gases and the ribbon is Mylar. Fargo recommends the shredding of printer ribbons using cross-cut shredding equipment (similar to that used for destroying video tapes). The material safety data sheet prepared for us Jan 3, 1999 by the ribbon manufacturer identifying the hazardous and non-hazardous materials can be found on the RAPIDS Training Resource CD-ROM.

## 6.10 Alternate Identification Numbers

There are many reasons that a sponsor or family member may not have an SSN as their primary identifier in DEERS. Besides the Service Number assigned to service members prior to 1967, members of foreign military, civilian contract employees, and family member may not be identified in DEERS with an SSN. These individuals may be entered into DEERS using a Service Number, Temporary Identification Number (TIN), Foreign Identification Number (FIN), or Civilian Identification Number (CIN).

**Note:** Without connectivity to DEERS, sites do not have the capability to generate these alternate identifiers. Cards using alternate identifiers cannot be produced when offline.

### 6.10.1 Temporary Identification Numbers

RAPIDS will issue a TIN to eligible family members who do not have valid SSNs. In the Add Dependent Navigator, when prompted to input the Person Identifier, the VO should select **None**. As the family member's information is saved to DEERS, a unique TIN is generated. When the automated ID card is issued, the letter **D** will print before the TIN in the family member's SSN field. The DD Form 1172 will also print the TIN.

A connection to DEERS is required to issue an ID card if a family member does not know or have his/her SSN. When issuing an ID card, RAPIDS needs to identify the individual on DEERS and in the ID card's bar code. While online, DEERS performs this function and generates the TIN automatically. The TIN is added on the ID card's bar code.

### 6.10.2 Foreign Identification Numbers

Certain categories of foreign personnel who are added to the DEERS database do not have SSNs. The RAPIDS software will issue a foreign identification number for this category. Refer to the Interservice publication when adding accompanying family members for the Foreign Military sponsor.

### 6.10.3 Civilian Identification Numbers

Civilian contract employees may be assigned a CIN in lieu of their SSN upon request. The CIN is a unique 9-digit number automatically generated by RAPIDS. All other government employees must supply their SSN's for entry into DEERS.

---

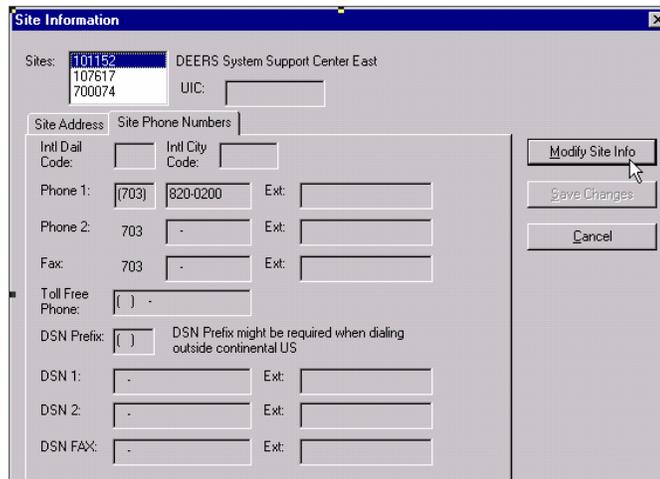
## 6.11 Using the Tools Menu

The **Tools** menu contains functions for changing your password, performing site and user administration, generating reports, configuring RAPIDS devices, and setting workspace preferences.

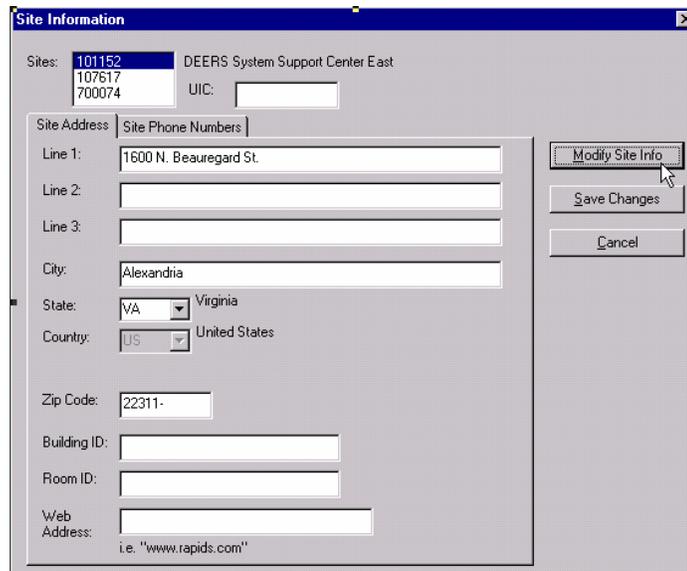
### 6.11.1 Site Information

Maintenance of an up-to-date and accurate site address and phone number is a key responsibility of the SSM. To modify your RAPIDS site address and/or UIC, use the Site Info function under the Tools menu. The following steps illustrate this process:

1. Open *Site Info* from the *Tools* menu.
2. Review the site information, addresses and phone numbers, to insure accuracy. Note the additional site address and phone number fields.



3. To add site information in the additional fields or make a correction to current information, click the Modify Site Info button. Note that you will not be able to modify the site name, city, or state.



4. Once corrections or changes have been completed and checked, click the **Save Changes** button.

To ensure consistency and accuracy of site information, all RAPIDS Site Name, city or state change requests must be routed through the appropriate DEERS/RAPIDS SPO listed in *Appendix C* of this guide.

### 6.11.2 DD Form 1172 Remarks List Updates

Each site's list of DD Form 1172 remarks is maintained on the RAPIDS server. The **Tools|DD Form 1172 Remarks** menu bar command gives SVOs access to their list of remarks so that they can add, delete, or modify any additional remarks to the list of standard RAPIDS remarks.

Adding to the remarks list can be quite helpful. For instance, if a Service command or local policy requires that a particular non-standard remark be included on DD Forms 1172, the remark could be added to the list. It can then be selected as a default remark to ensure that it is always included on DD Forms 1172.

### 6.11.3 User Administration

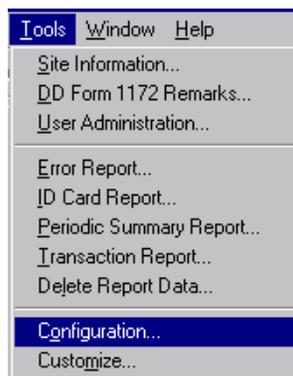
This option is detailed in *Section 9.2* of this training guide.

### 6.11.4 Reports

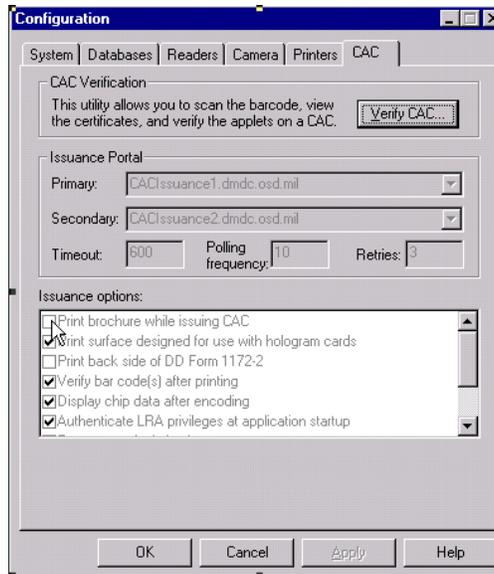
These options are detailed in *Section 8.4* of this training guide.

### 6.11.5 Configuration

The Configuration tool is used to obtain information via the **System, Authentication, Databases, Readers, Camera, Printers, and CAC** tabs. All users can view the **Configuration** option. Updates are restricted to RAPIDS SSMs under the direction of the D/RAC / D/RSC-E / DSO-A. Select the **Tools|Configuration** function to enter the **Configuration** tool.



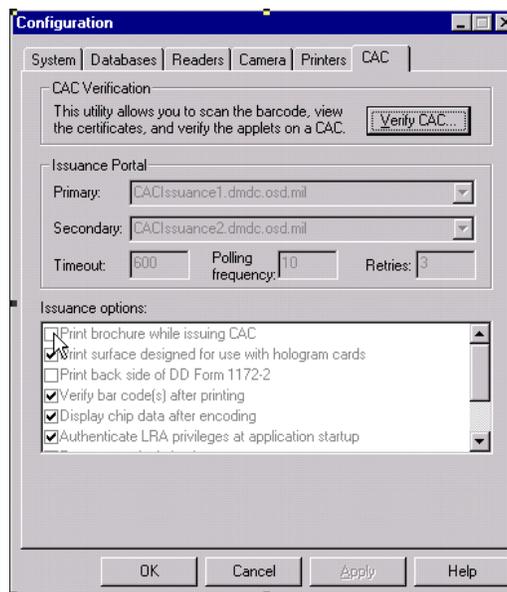
The **CAC** tab contains the CAC Verification Utility that allows the VO to scan the bar code, view the certificates, and verify information on the RAPIDS CAC. It is necessary to insert the CAC requiring verification into the CAC reader/encoder. Select the **Verify CAC** button to view the following additional tabs.



### 6.11.6 Printing the CAC Brochure

The site is responsible for providing the CAC brochure to every CAC recipient. Initially, a supply of brochures was shipped with the RAPIDS start-up supplies. Once the initial supply is depleted, the brochure can be printed through RAPIDS.

1. Select the *CAC* tab and the checkbox for **Print brochure while issuing CAC**.



### 6.11.7 Customize

“Customize” allows the user to customize preferences and DD Form 1172 defaults. It includes

*General*, *Main Window*, *Control*, and *Navigator* tabs. It is strongly suggested that the General, Menus and Toolbar, and Control tabs remain configured with the default settings. In the event that default settings have been altered and need to be reset, the VO should select the **Reset Tool Bars** button in the *Main Window* tab or the **Reset** button in the *Navigator* tab, as appropriate. The *Navigator* tab shows options for each navigator available in RAPIDS. Each user should update the DD Form 1172 Navigator using the following procedure for every workstation.

1. From the main menu, select **Tools|Customize**.
2. Select the *Navigator* tab.
3. Select **DD Form 1172** from the Navigator Name field drop-down list.
4. Under Default Official(s) (lower portion of the window), place a checkmark (√) in the appropriate boxes for VO and IO.
5. Click the block to the right of the Verifying field [which displays an ellipses (...)] to change the VO's name. At Select Official window, select the VO to be used as the default, then select **OK**.
6. If necessary, repeat the same procedure for selecting the default IO.

**Note:** Each user must complete this procedure for each RAPIDS workstation used by them.

---

## 6.12 RAPIDS Site Locator

The RAPIDS Site Locator is an online tool that displays the address and phone number of RAPIDS locations across the country. Because this tool uses the site information stored in DEERS, it is important that SSMs check this web site for accuracy. If inaccurate, the SSM must inform the DMDC Webmaster listed on the RAPIDS Site Locator of the inaccuracy and provide the correct information. The SSM must also use the RAPIDS **Tools|Site Address** function to correct site contact and address information. To access the RAPIDS Site Locator:

1. Select and open Microsoft Internet Explorer or another World Wide Web browser from an internet-connected computer.
2. Type in the Uniform Resource Locator (URL) of <http://www.dmdc.osd.mil>. This will take the user to the DMDC homepage.
3. Select the RAPIDS site locator (rabbit)  icon on the left navigation frame. This application is used to find the locations of ID card offices.
4. Chose a search method.



5. Enter the search criteria to generate a list of sites that most closely match your criteria.

---

### 6.13 Printing Selected Views from RAPIDS

The different views for a person or an entire family can be printed. The user must first choose from three options, and highlight the desired view.

1. To print the Address, Characteristics, and Benefits for the entire family, highlight the Sponsor's Identifier.
2. To print the Address, Characteristics, and Benefits for a single individual, highlight the individual's name.
3. To print only the Address, Characteristics, or Benefits views, highlight the specific view.

After the user has highlighted the correct Sponsor Identifier, individual, or view, select **File|Print|Selected View** from the main menu to get a hard copy. In addition, the user can also right-click the highlighted item and select **Print** from the drop-down list. It is not an actual screen print, because the printout does not look exactly like the screen.

---

### 6.14 Screen Printing through RAPIDS and Windows

If an actual printout of the screen is needed to capture error messages, follow the instructions below.

1. At the desired screen, press the PRINT SCREEN key (top row on the keyboard).
2. Click **Start** in the lower left corner of your screen.
3. Select **Programs|Accessories|Wordpad**.
4. At the WordPad desktop, select **Edit|Paste** from the menu. The desired screen appears within the WordPad program.
5. From the menu bar, select **File|Page Setup** and ensure that the "landscape orientation" is selected. Click **OK**.
6. From the menu bar, select **File|Print** to print the screen.
7. After the screen is printed, select **File|Exit** from the menu bar to close the application.

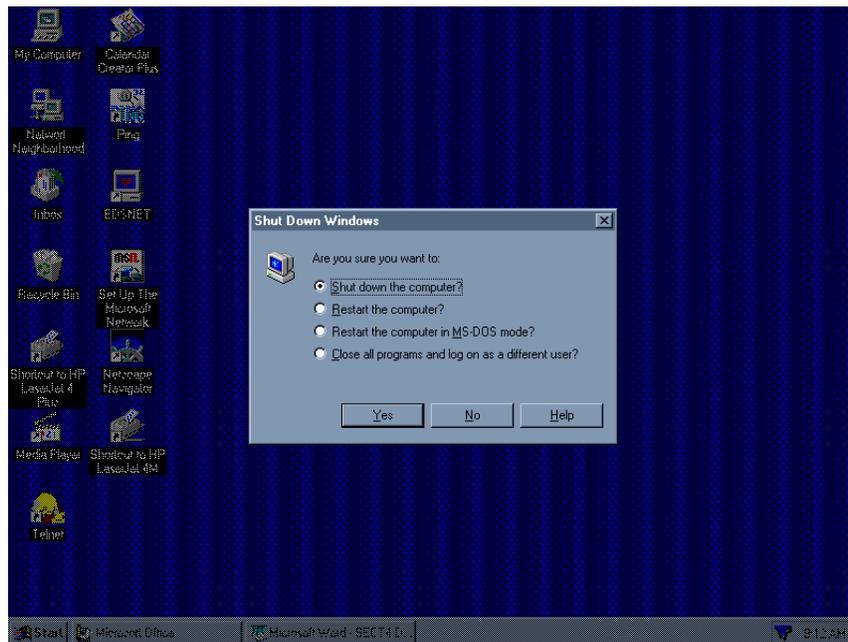
## 6.15 Shutting Down Your RAPIDS Workstation

Never turn off your computer while RAPIDS or Windows is still running. VOs must use proper shut down procedures at DEERS/RAPIDS workstations. The use of improper shut down procedures causes system "hard crashes" and creates great expense to the Department of Defense.

Please follow these steps when shutting down your RAPIDS workstation:

To close RAPIDS, select **File** then **Exit** from the main menu. Please be patient while the connection to the Issuance Portal closes. This may take several minutes. Next, disconnect your communications to the RAPIDS server (if appropriate). Ensure your CAC remains in the VO reader as you proceed to shut down Windows.

Shut down Windows by clicking **Start** from the taskbar and selecting the **Shut Down** command. A dialog box entitled *Shut Down Windows* appears. To shut down the system, **select Shut down the computer?** and click **Yes**. Your computer will display a message telling you when it is safe for you to shut off your computer. This may take several minutes due to NSA requirements to clear the memory prior to shutting down. Be patient! Turn off your computer, monitor, and peripherals via the surge suppressor switch only when your screen states that it is safe to shut down.



*Windows NT Shut Down Window*

**Note: NEVER shut down or power off the RAPIDS server (located at the RAPIDS server site) unless specifically instructed to do so by the D/RAC / D/RSC-E / DSO-A. Shutting down the RAPIDS server disables any of the connected RAPIDS workstations from using RAPIDS in either online or offline mode.**

## 7 Training Scenarios

This chapter illustrates step-by-step instructions for common situations with which the user may be faced when using RAPIDS. There are several ways of completing the below tasks. You may refer to *Section 6* of this training guide for assistance.

---

### 7.1 Add a New Family to DEERS

1. Select the **New Family** command from the **File** menu or the toolbar button. Effective 28 Feb 03, VO/LRAs will no longer be allowed to initially enter military members into the DEERS data base from RAPIDS workstations. The following steps can be completed by users with the Project Officer's role.
2. Type the Sponsor's Identifier and select **Enter**.
3. The Add Sponsor Navigator will walk the user through the steps necessary to add a new sponsor to the DEERS database.
4. Enter Sponsor's Personnel Category and any applicable Continuation Options. Select **Next**.
5. Enter Name and Marital Status. Select **Next**.
6. Enter Date of Birth, Gender, and Physical Attributes. Select **Next**.
7. Select Sponsor's Service Branch, Rank, Pay Grade, and enter Eligibility Date of Accession and Date of Termination. Select **Next**.
8. Enter Current Home Address and Phone Numbers and the Effective Date. Select **Finish**.
9. On Summary, select **Finish**.
10. Continuation Options to Add Dependents, Create a DD Form 1172, or Create an ID Card will guide the user to other navigators for these additional functions.
11. When all modifications to the family are completed, select the Save Family  icon from the main toolbar.

---

### 7.2 Add Family Members

1. Open Family.
2. Select Add Dependent Navigator from the main menu or main toolbar. The Add Dependent Navigator will walk the user through the steps necessary to add family members to the DEERS database.

3. Enter Dependent's Current Relationship, Person Identifier, Date of Birth, and any applicable Continuation Options. Select **Next**.
4. Enter Name, Gender, and Physical Attributes. Select **Next**.
5. Select any applicable Eligibility Conditions. Select **Next**.
6. Enter Current Home Address and Phone Numbers and the Effective Date. Select **Finish**.
7. On Summary, select **Finish**.
8. Repeat steps 2-7 for each dependent to be added.
9. Select the Save Family  icon from the main toolbar if you are finished modifying this family's data.

**Note:** Whenever you retrieve an existing family record, you should verify the address and telephone number information for the sponsor and each dependent, making corrections as necessary before performing other tasks.

---

### **7.3 Update a Family Member Over 21 to Reflect Student Status**

1. Open Family.
2. Open Dependent's **Characteristics** view.
3. On the **Student/Incap.** tab, click **Add Student/Incap.**
4. Select **Full-time Student** and enter Condition Begin and End Dates. Select **Finish**.
5. On Summary, select **Finish**.
6. Select the Save Family  icon from the main toolbar if you are finished modifying this family's data.

**Note:** If the ID card is issued within six months of the student's twenty-first birthday, the ID card will expire on the expected date of graduation or the day before the twenty-third birthday, whichever comes first. If the member requests the student ID card before the student is within six months of their twenty-first birthday, the ID card expiration date will be the day before the twenty-first birthday. This would require the student to return to the ID card section for issuance of a new ID card through the twenty-third birthday or expected graduation date, whichever comes first.

---

### **7.4 Update a Sponsor's Rank/Update Sponsor from Enlisted to Warrant Officer/Officer Rank with No Break in Service**

1. Open Family.

2. Open **Service Record** view.
3. On the **Branch, Rank, Pay Grade** tab, select the appropriate Rank and Pay Grade.
4. Enter the Effective Date of the change.
5. Select the Save Family  icon from the main toolbar.

**Notes:** If there is no break in service, DO NOT terminate the personnel category.

If the sponsor changes the Branch of Service, the previous category must be terminated and the new category with new Branch of Service added.

---

## 7.5 Update a Military Sponsor's Marriage Status to Reflect a Joint Service Marriage

**Note:** Joint Service Marriage (JSM) indicates whether a sponsor is married to another sponsor. As new populations such as DoD Civilians and Contractors are added to DEERS, the JSM rules could be expanded to include these populations. Sites should refer to regulation updates on a regular basis. Current regulations do not support enrolling dependents under more than one sponsor in a JSM for the same benefits. Exception: The Family Member Service Group Life Insurance (FMSGSLI) Program, effective 1 Oct 2001. Requires military spouses' to be enrolled under each other's DEERS record to established the "relationship" condition, before electing to receive, reduce, or decline the FMSGSLI benefit.

### 7.5.1 Update a JSM Sponsor to Become a Dependent Spouse Under the Other Sponsor's Record

This scenario can be used for any military JSM family or family member that becomes dependent entitled under the other benefit entitled sponsor. Situations include the following scenarios.

- **Both Active Duty:** when each sponsor shows their Active Duty spouse in RAPIDS, the spouses of service members can be automatically enrolled in the spousal version of the Service members Group Life Insurance (SGLI) benefit.
  - **When an Active Duty Sponsor Retires:** one member retires and becomes a dependent under the other Active Duty record (there may be occasions when one Active Duty sponsor may be entered under another Active Duty sponsor in JSMs).
  - **Guard/Reserve on Active Duty and Guard/Reserve spouse:** the Guard/Reserve spouse is authorized a dependent ID card under the spouse that is on Active Duty.
  - **JSM:** one spouse separates or is terminated from the military and is entitled to dependent benefits under the other spouse.
1. Open the record for the first sponsor.
  2. Open **Characteristics** view.

3. On the *Sponsor Specific* tab, ensure the marital status reflects Married.
4. Update the sponsor's **Service Record** view to reflect the appropriate Personnel Category (according to the documentation). You may want to expound on this area, or give an example or two as to what type of documentation we are referring to.
5. Add spouse to the record. (Refer to *Section 7.3* of this training guide). Notice the system automatically sets the benefits start date as the date of marriage or the sponsor's service start date. This date should be the day after the spouse retired, separated, or was terminated within the spouse's DEERS record.
6. To correct the benefits start date, open the spouse's **Characteristics** view.
7. On the *Relationship Condition* tab, click **Add Relationship Condition**.
8. Select "Terminate Entitlements Under Sponsor," enter the marriage date or the "active" sponsor's start date in the military (whichever is later) for the Date Ended Dependency. Deselect the Unknown checkmark for the end date, and enter the date of termination, separation, or retirement in the end date field. Select **Finish**. This step is especially important for Active Duty members who are married. Adding this Personnel Condition will ensure that the spouse (who is also an Active Duty sponsor) does not show benefits as a spouse.
9. On Summary, select **Finish**.
10. Select the Save Family  icon from the RAPIDS toolbar.
11. Open the second sponsor's record and repeat steps 2-10 to add the first sponsor as a spouse.

**Note:** Steps 6-9 erase all benefits associated to the spouse's record prior to the actual start date of the spouse dependency.

### 7.5.2 Terminate a Dependent Under One Sponsor and Add Under Another

1. Open the Sponsor record that currently lists the dependent.
2. Open the Dependent's **Characteristics** view.
3. On the *Relationship Condition* tab, click **Add Relationship Condition**.
4. Select **Terminate Entitlements Under Sponsor** and enter Date ended Dependency. Select **Finish**.
5. On Summary, select **Finish**.
6. Select the Save Family  icon from the main toolbar.
7. Open the Sponsor's record to which the dependent is to be added.

8. Add the dependent to the record. (Refer to *Section 7.3* of this training guide).

**Note: When moving family members from one record to another, be careful when entering the start and end dates.** Dependency for the new sponsor should start the day after the end of the current one. This will ensure that there is no break in coverage and no double or overlapping periods of coverage.

When enrolling a child under the Active Duty sponsor for Medical benefits and the Guard/Reserve sponsor for Reserve Dental Program Benefits, the relationship condition of **Terminate Entitlements Under Sponsor** does not need to be added.

### **7.5.3 Transfer Children/Update entitlements between Sponsors in a JSM or Under Active Duty Sponsors**

This scenario can be used for updating the entitlements of a child who may be eligible for benefits under one or the other Active Duty parent or as a stepchild of another military sponsor. Current regulations do not support enrolling dependents under more than one sponsor for the same benefits. It is important to ensure that the childrens' entitlement begin and end dates do not show overlapping periods of coverage or periods without coverage.

Example: Child is enrolled under Active Duty Sponsor A from date of birth (1990Jan01). Sponsor A requests this same child's DEERS entitlements ended on 1995Feb01 so child can be enrolled under Active Duty Sponsor B as a dependent. In 2000Mar01 Active Duty Sponsor B wishes to move the child back to Sponsor A in DEERS.

1. Open the record for the Sponsor A.
2. Verify that child has been added as a dependent to Sponsor A's record. If child does not appear, add child to record (Refer to *Section 7.3* of this training guide).
3. To terminate entitlements for this child under Sponsor A, select the **Relationship Condition** tab from the **Characteristics** view. Click **Add Relationship Condition**. The relationship of Child will remain intact, only the entitlements will be terminated.
4. Select "Terminate Entitlements Under Sponsor." At the "Date ended Dependency" field, enter the last date that the child will receive the entitlements through Sponsor A. The unknown end date can remain. Select **Finish**.
5. On Summary, select **Finish**. You have now terminated all entitlements for this child under Sponsor A.
6. To add the child and continue entitlements under Sponsor B, open the record for Sponsor B.
7. Add the child as a dependent to Sponsor B's record (refer to *Section 7.3* of this training guide).
8. Select the **Relationship Condition** tab from the **Characteristics** view. Click **Add Relationship Condition**. The RAPIDS rules default the child's eligibility coverage to the

child's date of birth or the sponsor's start date (which ever is later). Since this child was previously receiving entitlements under another sponsor, it is necessary to terminate the entitlements under Sponsor B for the time that the child was receiving entitlements through Sponsor A.

9. Select "Terminate Entitlements Under Sponsor." At the "Date ended Dependency" field, enter the child's date of birth and last date that the child was enrolled under Sponsor A. Select **Finish**
10. On Summary, select **Finish**.
11. Select the Save Family  icon from the main toolbar.

**Note: When moving family members from one record to another, be careful when entering the start and end dates.** Dependency for the new sponsor should start the day after the end of the current one. This will ensure that there is no break in coverage and no double or overlapping periods of coverage.

When enrolling a child under the Active Duty sponsor for Medical benefits and the Guard/Reserve sponsor for Reserve Dental Program Benefits, the relationship condition of **Terminate Entitlements Under Sponsor** does not need to be added.

#### 7.5.4 Terminate a Dependent Under One Sponsor and Add Under Another

1. Open the Family record that currently lists the dependent.
2. Open the Dependent's **Characteristics** view.
3. On the **Relationship Condition** tab, click **Add Relationship Condition**.
4. Select **Terminate Entitlements Under Sponsor** and enter Date ended Dependency. Select **Finish**.
5. On Summary, select **Finish**.
6. Select the Save Family  icon from the main toolbar.
7. Open the Sponsor's record to which the dependent is to be added.
8. Add the dependent to the record. (Refer to *Scenario 6.3*).

**Note: When moving family members from one record to another, be careful when entering the start and end dates.** Dependency for the new sponsor should start the day after the end of the current one. This will ensure that there is no break in coverage and no double coverage.

## 7.6 Divorce a Sponsor from a Spouse Who Does Not Meet Unremarried Former Spouse Requirements

1. Open Family.
2. Open Spouse's **Characteristics** view.
3. On the **Relationship** tab, click **Terminate Relationship**.
4. Select **Separation**. Select **Next**.
5. Select **Divorce** for the Termination Reason and enter End Date. Select **Next**.
6. At the Former Spouse Qualification screen, select **Finish** since spouse does not meet requirements.

**Note:** Former Spouse Qualification requires proper documentation (that is, statement of service, complete set of DD Forms 214 prior to completing this verification).

7. On Summary, select **Finish**. The benefits will disappear.
8. Select the Save Family  icon from the main toolbar.

**Note:** If spouse does not meet the URFS requirement, the qualification screen is not required. When terminating a spouse for divorce, the initial verification of Former Spouse must be determined by the parent Service. Users should not complete the Former Spouse "Qualification Screen" without proper documentation. While waiting for verification of sponsor's Service (i.e., statement of service, complete set(s) of DD Forms 214), a temporary ID card may be issued with the following expiration dates if the former spouse appears to be eligible: 120 days for former spouse of a retiree; 30 days for Active Duty. The former spouse should acknowledge in item 89 on the DD Form 1172 that he or she has not remarried or enrolled in an employer-sponsored health plan and that he or she will also be responsible for any medical care received during this period if found ineligible for an ID card.

---

## 7.7 Divorce a Sponsor from a Spouse Who Meets URFS Requirements

1. Open Family.
2. Open Spouse's **Characteristics** view.
3. On the **Relationship** tab, click **Terminate Relationship**.
4. Select **Separation**. Select **Next**.
5. Select **Divorce** for the Termination Reason and enter End Date. Select **Next**.
6. Complete the Former Spouse Qualification screen with the following conditions. Enter number of years of marriage, whether sponsor's length of service is at least 20 years, and

number of years marriage overlaps with sponsor's years of service. If applicable, check **Eligible for transition compensation** or **Has other health insurance**. Select **Finish**.

7. On Summary, select **Finish**. Relationship will show as Former Spouse with benefits.
8. Select the Save Family  icon from the main toolbar.

**Note:** When terminating a spouse for divorce, the parent Service must determine the initial verification of a Former Spouse. Users should not complete the Former Spouse “Qualification Screen” without proper documentation. While waiting for verification of sponsor's service (i.e., statement of service, DD Forms 214), a temporary ID card may be issued with the following expiration dates if the former spouse appears to be eligible: 120 days for former spouse of a retiree; 30 days for Active Duty. The former spouse should acknowledge in item 89 on the DD Form 1172 that he or she has not remarried or enrolled in an employer-sponsored health plan and that he or she will also be responsible for any medical care received during this period if found to be ineligible for an ID card.

---

## 7.8 Update a Child who is living with an Ex-Spouse

1. Open Family.
2. Open Child's **Characteristics** view.
3. On the **Relationship Condition** tab, click **Add Relationship Condition**.
4. Select **Sponsor provides over 50% support** and enter Date Moved Out of Sponsor's Household. Select **Finish**.
5. On Summary, select **Finish**.
6. Update child's address.
7. Select the Save Family  icon from the main toolbar.

**Note:** Benefits now reflect that the child no longer has commissary benefits.

---

## 7.9 Retire an Active Duty Sponsor

1. Open Family.
2. Open **Service Record** view.
3. On the **Personnel Category** tab, click **Terminate Personnel Category**.
4. Select **Retirement**. Select **Next**.
5. Enter **Other** for Retirement Type and Date of Retirement. Select **Finish**.

6. On Summary, select **Finish**.
7. Select the Save Family  icon from the main toolbar. Both Active Duty and Retired statuses may show in the Family Tree and Service Record.

---

### 7.10 Update Active Duty Sponsor to Temporary Disabled Retirement List (TDRL)

1. Open Family.
2. Open **Service Record** view.
3. On the *Personnel Category* tab, click **Terminate Personnel Category**.
4. Select **Retirement**. Select **Next**.
5. Enter **Temp. Disabled List** for Retirement Type and Date of Retirement. Select **Finish**.
6. On Summary, select **Finish**.
7. Select the Save Family  icon from the main toolbar. Both Active Duty and Retired statuses will show in the Family Tree and Service Record.

**Note:** RAPIDS will extend the card expiration date to five years. The user must change the expiration date (in Create ID Card Navigator) from the default five years to 30 months from the date the member was placed on the TDRL. After the initial-30 month issue period, the card should be reissued for an additional 30 months. If the member is not eligible for Medicare Part A at the end of the first 30-month period, the VO should reissue the card in one-year intervals for a maximum of five years from the date the member was placed on TDRL (AFI 36-3026).

---

### 7.11 Update TDRL Sponsor to Permanently Disabled Retired List (PDRL)

1. Open Sponsor.
2. Open **Retired Service Record** view.
3. On the *Personnel Condition* tab, click **Add Personnel Condition**.
4. Select **TDRL to PDRL** and enter Begin Date PDRL. Select **Finish**. (This condition allows the TDRL to PDRL date to be captured).
5. On Summary, select **Finish**.
6. The Family Tree and Service Record will display an additional status of Retired PDRL after TDRL.
7. Select the Save Family  icon from the main toolbar.

## 7.12 Terminate Sponsor for End of Contract

1. Open Sponsor.
2. Open **Service Record** view.
3. On the *Personnel Category* tab, click **Terminate Personnel Category**.
4. Select **Separation**. Select **Next**.
5. From the DD Form 214, enter SPD Code, Character of Service, and Date of Separation. Select **Finish**.
6. On Summary, select **Finish**.
7. Select the Save Family  icon from the main toolbar.

**Note:** To terminate a Guard/Reserve member, disregard step 5.

### 7.12.1 Terminate Sponsor for End of Contract and Revoke CAC

1. Open Sponsor.
2. Open **Service Record** view.
3. On the *Personnel Category* tab, click **Terminate Personnel Category**.
4. Select **Separation**. Select **Next**.
5. Use the DD Form 214 (as applicable) and enter the SPD Code, Character of Service, and Date of Separation. Select **Finish**. To terminate a DoD Civil Service or DoD contractor, select **Separation**, and enter the Date of Termination.
6. On Summary, select **Terminate**.
7. Select the Save Family  icon from the main toolbar.
8. Termination of the Personnel Category will terminate the CAC and revoke the associated certificates.

### 7.12.2 Terminate ID Card/CAC without Terminating the Personnel Category or Relationship

1. Open Sponsor.
2. On the Family Tree, highlight and right-click the card that must be terminated.
3. Select **Terminate . . .** from the Quick Action menu.

4. At the Terminate Card navigator, select the card termination date and the reason for termination (i.e., the card was lost).
5. On Summary, select **Finish**.
6. The card will be terminated. If a CAC was selected for termination, associated certificates will also be revoked.
7. Issue a replacement card using the Create Card navigator.

---

### 7.13 Separate Sponsor from Active Duty and Add to Guard/Reserves

1. Open Family.
2. Open **Service Record** view.
3. On the *Personnel Category* tab, click **Terminate Personnel Category**.
4. Select **Separation**. Select **Next**.
5. From the DD Form 214, enter the SPD Code, Character of Service, and Date of Separation. Select **Finish**.
6. On Summary, select **Finish**.
7. On the *Personnel Category* tab, click **Add Personnel Category**.
8. Select **National Guard** or **Reserve**. Select **Next**.
9. Enter Sponsor's Service Branch, Rank, and Pay Grade, and Contract Begin and End Dates. Select **Finish**.
10. On the *Other* tab, insure that the correct Reserve Component Category (RCC) is selected. If incorrect, click the Modify button and select the correct RCC and contract begin date.
11. On Summary, select **Create**. A Guard/Reserve card can now be issued.
12. Select the Save Family  icon from the main toolbar.

#### 7.13.1 RCC definitions:

1. *Individual Ready Reserve (IRR)*: mobilization-asset and non-mobilization-asset – The IRR (together with the Inactive National Guard), a manpower pool comprised mostly of trained individuals, having served previously on Active Duty or in the Selected Reserve. Also have a period of their Military Service Obligation remaining.
2. *Retired Reserve*, less than age 60

3. *Selected Reserve*: Trained unit members who participate in unit training on a part time basis.
4. *Standby Reserve*: Consist of personnel who maintain their military affiliation without being in the Ready Reserve. These individuals are not required to perform training and are not part of any unit.

VOs unsure as to which RCC to select should contact their SPO. A List of all SPOs can be found in *Appendix C*.

---

#### 7.14 Separate Sponsor and Issue Transition Assistance (TA), Voluntary Separation Incentive (VSI), or Special Separation Benefit (SSB) and Guard/Reserve ID Cards

1. Open Family.
2. Open **Service Record** view.
3. On the *Personnel Category* tab, click **Terminate Personnel Category**.
4. Select **Separation**. Select **Next**.
5. From the DD Form 214, enter the SPD Code, Character of Service, and Date of Separation. Select **Finish**.
6. On Summary, select **Finish**.
7. On the pop-up dialog box, enter the Length of Service in years and months, and select **OK**. (This box may not appear if RAPIDS can determine the Length of Service.)
8. Open **Active Duty-TA Service Record**. A TA card can now be issued.  
**Note:** The Create ID Card Navigator will walk the VO through issuing a new DD Form 2765 for the TA sponsor. Eligible family members will continue to receive the DD Form 1173.
9. To issue a Guard/Reserve card, select the Reopen Family  icon from the main toolbar.
10. Open **Service Record** view.
11. On the *Personnel Category* tab, click **Add Personnel Category**.
12. Select **National Guard** or **Reserve**. Select **Next**.
13. Enter the Sponsor's Service Branch, Rank, and Pay Grade, and Contract Begin and End Dates. Select **Finish**.
14. On Summary, select **Finish**. A Guard/Reserve ID card can now be issued.
15. Select the Save Family  icon from the main toolbar.

### 7.15 Issue ID Card for TA Sponsor or Family Member(s) After Medical Eligibility Has Expired

1. Open Family.
2. Select **ID Card Navigator** from the main menu or main toolbar.
3. Select Sponsors' or Family Members' TA card. Select **Next**.

**Note:** If the DEERS Service Record does not reflect the TA condition, the VO will need to add a condition of TA to establish correct medical, commissary, exchange, and MWR privileges.

4. Re-take the photograph and select **OK**.
5. On Summary, select **Finish**.
6. Print ID card.

---

### 7.16 Extend Guard/Reserve Contract End Date for Guard/Reserve Sponsor

1. Open Family.
2. Open **Service Record** view.
3. On the **Personnel Category** tab, input new End of Contract Date
4. On the **Other** tab, insure that the correct Reserve Component Category (RCC) is selected. If incorrect, click the Modify button and select the correct RCC and contract begin date.
5. Select the Save Family  icon from the main toolbar.
6. Proceed to DD Form 1172 and ID Card Navigators to issue new DD Form 1172 and ID card.

**Note:** The end of contract or mandatory removal date for enlisted Guard/Reserve personnel cannot be more than 10 years in the future.

---

### 7.17 Activate a Guard/Reserve Sponsor

1. Open Family.
2. Open **Service Record** view.
3. On the **Personnel Condition** tab, click **Add Personnel Condition**.
4. Select **On Active Duty** for Personnel Condition and enter Active Duty Begin and End Dates. Select **Finish**.

**Note:** If sponsor is being activated for Special Operations, select the Special Operation from the drop down list as indicated on the orders.

5. On Summary, select **Finish**.
6. Select the Save Family  icon from the main toolbar. Both Reserve/Guard and Reserve/Guard on Active Duty statuses will show in the Family Tree and Service Record.

**Note:** Begin date of activation must be within 14 days of issue date.

---

### 7.18 Extend Active Duty End Date for a Guard/Reserve Sponsor

1. Open Family.
2. Open **On Active Duty Service Record** view.
3. On the *Personnel Condition* tab, input new Active Duty End Date.
4. On the *Other* tab, insure that the correct Reserve Component Category (RCC) is selected. If incorrect, click the Modify button and select the correct RCC and contract begin date.
5. Select the Save Family  icon from the main toolbar.
6. Proceed to DD Form 1172 and ID Card Navigators to issue new DD Form 1172 and ID card.

---

### 7.19 Deactivate a Guard/Reserve Sponsor

1. Open Family.
2. Open **On Active Duty Service Record** view.
3. On the *Personnel Condition* tab, click **Terminate Personnel Condition**.
4. Select **Separation** and enter Date of Separation. Select **Finish**.  
**Note:** Separation attributes (SPD Code, Reenlistment Code, and Character of Service) are not required to complete this operation.
5. On Summary, select **Finish**.
6. Select the Save Family  icon from the main toolbar.

---

### 7.20 Separate Guard/Reserve Sponsor Involuntarily from the Selected Reserves

1. Open Family.
2. Open **Service Record** view.

3. On the *Personnel Category* tab, click **Terminate Personnel Category**.
4. Select **Separation**. Select **Next**.
5. Enter the SPD Code from the DD Form 214. If no DD Form 214 was issued, enter a SPD Code of **LTT**, Character of Service of **Honorable**, and Date of Separation or Reassignment. Select **Finish**.
6. On Summary, select **Finish**.
7. If prompted by the pop-up dialog box, enter Selective Reserves Separation Date. A Selected Reserves Transition Assistance (TA-RES) ID card can now be issued.
8. Select the Save Family  icon from the main toolbar.

---

### 7.21 Update Inactive Ready Reserve (IRR) to Selected Reserves

1. Open Family.
2. Open **Service Record** view.
3. On the *Other* tab, select **Modify** on the Reserve Component Category field.
4. Select the Selected Reserve Component category, and enter the begin date. Select **OK**.

---

### 7.22 Separate Guard/Reserve Sponsor from an Active Duty Mobilization

1. Open Sponsor.
2. Open **Special Operation Condition** view.
3. On the *Personnel Condition* tab, click **Terminate Personnel Condition**.
4. Select **Separation** and enter Date of Termination. Select **Finish**.
5. On Summary, select **Finish**.
6. On the pop-up dialog box, answer **Yes** or **No** to the question “Is the mobilization condition being terminated due to a Federal Act?” If yes is selected, a TA card can now be issued.
7. Select the Save Family  icon from the main toolbar.

---

### 7.23 Transfer Guard/Reserve Sponsor from One Branch of Service to Another (e.g., Army Reserve to Air National Guard)

1. Open Family.

2. Open **Guard/Reserve Service Record** view.
3. On the *Personnel Category* tab, click **Terminate Personnel Category**.
4. Select **Separation**. Select **Next**.
5. Enter Date of Separation. Select **Finish**. Date of Separation should be one day prior to date of new enlistment of gaining organization.
6. On Summary, select **Finish**.
7. Click **Add Personnel Category**.
8. Select **National Guard** or **Reserve**. Select **Next**.
9. Select new Service Branch, Rank, Pay Grade, and Contract Begin and End Dates for the new enlistment. Current Contract Begin Date must be at least one day after the Date of Separation. It may be necessary to scroll up/down to select the appropriate Branch of Service. Select **Finish**.
10. On Summary, select **Finish**.
11. Select the Save Family  icon from the main toolbar.

---

#### 7.24 Retire a Guard/Reserve Sponsor under the Age of 60 to Reflect Reserve Retired Category

1. Open Family.
2. Open **Service Record** view.
3. On the *Personnel Category* tab, click **Terminate Personnel Category**.
4. Select **Retirement**. Select **Next**.
5. Enter Retirement Type, Date of Retirement, and select **Awaiting Retirement at Age 60**. Select **Finish**.
6. A message will display warning the user that the “sponsor was marked as RESRET and therefore will not be retired with full retirement benefits.” Select **OK**.
7. On Summary, select **Finish**.
8. Select the Save Family  icon from the main toolbar.

**Note:** A URFS of a Reserve retiree is not entitled to benefits until the sponsor reaches age 60.

### 7.25 Retire an Active Guard/Reserve Sponsor with Benefits and Pay Before Age 60

1. Open Family.
2. Open **On Active Duty Service Record** view.  
**Note:** If the date of separation for the On Active Duty condition and the National Guard or Reserve category are the same, skip to step 8. This will terminate both the category and condition with one step.
3. On the *Personnel Condition* tab, click **Terminate Personnel Condition**.
4. Select **Separation**. Select **Next**.
5. Enter Date of Separation. Select **Finish**.
6. On Summary, select **Separate**.
7. Select **Guard/Reserve Service Record** view.
8. On the *Personnel Category* tab, click **Terminate Personnel Category**.
9. Select **Retirement**. Select **Next**.
10. Enter Retirement Type, Date of Retirement. Deselect **Awaiting Retirement at Age 60** box. Select **Finish**.
11. A message will display warning the user that the “sponsor was NOT marked as RESRET and therefore will be retired with full retirement benefits.” Select **OK**.
12. On Summary, select **Finish**.
13. Select the Save Family  icon from the main toolbar.

---

### 7.26 Change Reserve Retired Sponsor to Reflect Retired Category at Age 60 or Over

1. Open Family.
2. Open **Service Record** view.
3. On the *Personnel Category* tab, click **Terminate Personnel Category**.
4. Select **Retirement** and enter Retirement Type and the sponsor’s 60<sup>th</sup> birth date in Retirement Date. Select **Finish**.
5. On Summary, select **Finish**.
6. Select the Save Family  icon from the main toolbar.

### 7.27 Add Court-Ordered Ward/Pre-Adopt to Sponsor

1. Open Family.
2. Select **Add Dependent Navigator**.
3. Enter **Ward** for Dependent's Current Relationship, Person Identifier, Date of Birth, and any applicable Continuation Options. Select **Next**.
4. Enter Name, Gender, Physical Attributes, and Date of Sponsorship. Select **Next**.
5. Select any applicable Eligibility Conditions. Select **Next**.
6. Enter Current Home Address and Phone Numbers and the Effective Date. Select **Finish**.
7. On Summary, select **Finish**.
8. Ward will be added to sponsor record.
9. To complete as Court Ordered Ward/Pre-Adopt (and establish benefits), select the Ward's **Characteristics** view.
10. On the **Relationship Condition** tab, click **Add Relationship Condition**.
11. Select **Court Order** (this allows for Military Services Direct Care and Civilian Health privileges) and enter Condition begin date. Select **Finish**.
12. On Summary, select **Finish**.
13. Select the Save Family  icon from the main toolbar.

---

### 7.28 Change Relationship from Ward/Stepchild to Child When Sponsor Adopts the Ward/Stepchild

1. Open Family.
2. Open the Dependent's **Characteristics** view.
3. On the **Relationship** tab, click **Terminate Relationship**.
4. Select **Separation**. Select **Next**.
5. Select **Adoption by Sponsor** for Reason Relationship Being Terminated and enter End Date (date of adoption).
6. Select **Finish**.
7. On Summary, select **Terminate**.
8. Select the Save Family  icon from the main toolbar.

**Note:** The relationship of Ward or Stepchild will be terminated, and the relationship of Child will display. The start date for benefits will not change.

---

## **7.29 Medicare**

The FY2001 National Defense Authorization Act for Fiscal Year 2001, Public Law 106-398 (the Act) was signed into being October 30, 2000. The legislation included a number of health care provisions that collectively represent the most significant change to military health care benefits since the Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) was established by Congress in 1966.

Previously, if someone became Medicare Eligible on the first day of their 65th birthday, their TRICARE (or CHAMPUS) benefits would end. Under the new provisions, this has changed. Now, given specific requirements, these same people are entitled to maintain their Civilian Health benefits. This fact makes it more important than ever to insure that correct Medicare information is collected by the VO and entered in DEERS through RAPIDS.

When an individual is entitled to Medicare because of the basic Medicare rule (first day of the month that they become age 65), RAPIDS will continue to generate a default Medicare segment when appropriate. RAPIDS will base Civilian Health benefits on the person's age and Medicare rules. RAPIDS collects Medicare part A information that is an exception to the default. See below for each reason code.

When entering Medicare through the RAPIDS Application, the VO is actually entering one of two types of Medicare:

- Medicare Part A : Inpatient Medical Coverage
- Medicare Part B : Outpatient Medical Coverage

A vital piece of information needed when dealing with Medicare is the effective and end date of the enrollment to the Medicare Type. These dates outline when the individual is enrolled or not enrolled in Medicare. It is important to remember that the effective date and end date of Medicare Type A and Medicare Type B can and do flow independently of each other. As a general rule, eligibility effective dates fall on the first of the eligible month. There are exceptions to this rule.

The next piece of information that is needed when entering Medicare is a Medicare Reason. Remember that VO's should only enter exceptions to the default rule. Therefore, the Medicare Reason is the reason an exception is being added.

### **7.29.1 Medicare Part A Reason Codes**

- Not Eligible at age 65 – When entering this value the system is being told that the individual does not have enough quarters of Social Security contributions to qualify for Medicare benefits when the individuals Medicare Eligibility date is reached. The effective date of this Medicare Part A must be the individuals Medicare Eligibility date.
- Eligible After 65th Birthday – When entering this value the system is being told that the individual has reached the required quarters of Social Security contributions to qualify

for Medicare benefits some time after the individuals Medicare Eligibility date is reached. The effective date of this Medicare Part A must be after the individuals Medicare Eligibility date and should be preceded by a Medicare Part A reason of “Not Eligible at age 65”.

- Eligible because of Disability - When entering this value the system is being told that the individual is eligible for Medicare because of a disability. The effective date of this Medicare Part A must be before the individuals Medicare Eligibility date.
- Eligible because of End-Stage Renal - When entering this value the system is being told that the individual is eligible for Medicare because of an End-Stage Renal Disease. If and when a new kidney is obtained they will then be eligible to be dropped from Medicare eligibility. The effective date of this Medicare Part A must be before the individuals Medicare Eligibility date.
- Purchased - When entering this value the system is being told that the individual has purchased Medicare Part A. The effective date of this Medicare Part A must be on or after the individuals Medicare Eligibility date.

### 7.29.2 Medicare Part B Reason Code

- Enrollment in Part B -- When entering this value the system is being told that the individual has purchased Medicare Part B (outpatient Medical Coverage). The effective date of this Medicare Part B must be on or after the individual’s Medicare Eligibility date.

#### **The effects of these Medicare Types and Reasons on Civilian Health are as follows:**

- Default Medicare Rule - The individual loses eligibility to Civilian Health starting at their Medicare Eligibility date. Once Medicare Part B is added, Civilian Health eligibility as a secondary payer is returned to the individual for the duration of the Part B segment. **Note:** Civilian Health eligibility will be returned on the later of the Part B effective date or October 1 2001.
- Medicare Part A Reason “Not Eligible at age 65” – The individual remains eligible for Civilian Health for the entire duration of the Part A segment.
- Medicare Part A Reason “Eligible after 65th Birthday” – The individual loses eligibility to Civilian Health during the duration of the Part A. Once Medicare Part B is added, Civilian Health eligibility as a secondary payer is returned to the individual for the duration of the Part B segment. **Note:** Civilian Health eligibility will be returned on the later of the Part B effective date or October 1 2001.
- Medicare Part A Reason “Eligible because of Disability” and “Eligible because of End-Stage Renal” – The individual loses eligibility to Civilian Health during the duration of the Part A. Once Medicare Part B is added, Civilian Health eligibility as a secondary payer is returned to the individual for the duration of the Part B segment. **Note:** Civilian Health eligibility over 65 will be returned on the later of the Part B effective date or October 1 2001.
- Medicare Part A Reason “Purchased” – The individual remains eligible for Civilian Health for the entire duration of the Part A segment.

- Medicare Part B Reason “Purchased” -- Civilian Health eligibility as a secondary payer is available to the individual for the duration of the Part B segment. **Note:** Civilian Health eligibility will be returned on the later of the Part B effective date or October 1 2001.

**Note:** If dependent of an Active Duty (AD) sponsor is being updated, they will continue to receive Civilian Health regardless of their enrollment in Medicare Part B. See the Service Regulations for details.

### 7.29.3 Add Medicare Benefits for a Family Member under Age 65

1. Open Family.
2. Open Dependent’s **Other Contract Plans** view.
3. On the **Other Govt Programs** tab, click **Add Medicare**.
4. Enter **Medicare Part A** for Medicare Type, Medicare Begin Date, and Reason for Medicare. Enter Health Insurance Claim Number (HICN) when prompted. This may be found on the Medicare card. Select **Finish**.
5. On Summary, select **Create**. Medicare Part A information will be displayed.
6. Click **Add Medicare**.
7. If Medicare Part B has been purchased (making the family member entitled to Civilian Health), enter **Medicare Part B** for Medicare Type and Medicare Begin Date. (The reason field will be pre-filled with Purchased).
8. Select the Save Family  icon from the main toolbar.

### 7.29.4 Update Medicare Benefits for a Family Member Not Eligible for Medicare Part A After Age 65

1. Open Family.
2. Open dependent’s **Other Contract Plans** view.
3. On the **Other Govt Programs** tab, click **Add Medicare**.
4. Enter **Medicare Part A** for Medicare Type, Medicare Begin Date (the date Medicare would have started), and **Not eligible at age 65** for Reason for Medicare. Enter Health Insurance Claim Number (HICN) when prompted. This may be found on the Medicare card. Select **Finish**.
5. On Summary, select **Finish**.
6. Select the Save Family  icon from the main toolbar.

### 7.29.5 Update Medicare Benefits for a Family Member Not Eligible for Medicare Part A After Age 65, Purchasing Medicare Part B

1. Open Family.
2. Open dependent's **Other Contract Plans** view.
3. On the **Other Govt Programs** tab, click **Add Medicare**.
4. Enter **Medicare Part A** for Medicare Type, Medicare Begin Date (the date Medicare would have started), and **Not eligible at age 65** for Reason for Medicare. Enter Health Insurance Claim Number (HICN) when prompted. This may be found on the Medicare card. Select **Finish**.
5. On Summary, select **Finish**.
6. Again, click **Add Medicare**.
7. Enter **Medicare Part B** for Medicare Type, Medicare Begin Date, and Reason for Medicare of **Purchased** will automatically be selected. Select **Finish**.
8. On Summary, select **Finish**.
9. Select the Save Family  icon from the main toolbar.

### 7.29.6 Enter Medicare Part B for an aging in (turning age 65) beneficiary to reflect their TRICARE For Life Entitlement.

1. Open Family.
2. Open Sponsor or Dependent's **Other Contract Plans** view.
3. Review the recipient's Medicare Card. If Medicare Part B has been purchased, it will be displayed on the Medicare card.
4. On the **Other Govt Programs** tab, click **Add Medicare**.
5. Enter **Medicare Part B** for Medicare Type, the Medicare Begin Date as displayed on the Medicare card. The reason field will be pre-filled with **Purchased**. Enter Health Insurance Claim Number (HICN) when prompted. This may be found on the Medicare card. Select **Finish**.
6. On Summary, select **Create**. Medicare Part B information will be displayed.

Select the Save Family  icon from the main toolbar.

### 7.30 Issue Non-commissioned NOAA Personnel ID cards

1. Select **New Family** from the **File** menu.
2. Type the sponsor's identifier and select **Enter**.
3. The Add Sponsor navigator will guide the VO through the steps necessary to add a new sponsor to DEERS. Select **Other Federal Agency Employee** as the Personnel Category. Select **Next**.
4. Enter the sponsor's name and marital status. Select **Next**.
5. Enter the date of birth, gender, and physical attributes. Select **Next**.
6. Select the appropriate pay plan/grade or "Other". Enter the sponsor's date of employment, contract end date or retirement date. Select the Service/Org of NOAA. When selecting the Contract type, the RAPIDS Verifying Official will have four choices: Contract Surgeon, Member of the United Seaman's Service, NOAA Civilian Shipboard Crewman, or NOAA Civilian Shipboard Officer. Select the appropriate contract type from the list above. Select **Next**.
7. If the pay category of Other was selected, the VO is prompted to type the appropriate pay category. Enter the Geneva Conventions Category.
8. Enter the sponsor's home address, phone number, and e-mail address with effective dates. Select **Finish**.
9. On Summary, select **Finish**.

**Note:** Family members should not be added to DEERS unless receiving DoD benefits.

---

### 7.31 Graduate Service Academy to Active Duty

1. Open Family.
2. Open Service Record.
3. At the **Personnel Category** tab, select **Terminate Personnel Category**.
4. Select **Graduation**. Then, **Next**.
5. Branch, Rank, and Pay Grade are automatically chosen.  
**Note:** You may change Branch of Service at this point.
6. Enter the **Date of Accession** and the **Date of Termination**. Then, select **Finish**.
7. At the Summary screen, after verifying the information, select **Finish**.

8. Verify that the Academy Student record is terminated and that the Active Duty record is created.

---

## 7.32 Deceased Sponsor

### 7.32.1 Create Deceased Sponsor (When the Sponsor is Not Showing on DEERS) and Add Unremarried Widow/Widower

1. Attempt to Open Family to ensure that the sponsor is not already showing on DEERS.
2. Select **Yes** when the message appears stating, “The requested family was not found. Add new family to DEERS using the sponsor identifier?”
3. Enter Sponsor’s Personnel Category prior to death and any applicable Continuation Options. Select **Next**.
4. Enter Name and Marital Status prior to death. Select **Next**.
5. Enter Date of Birth, Gender, and Physical Attributes (Unknowns and Not Applicable may be used). Select **Next**.
6. Select Sponsor’s Service Branch, Rank, Pay Grade and Eligibility Date of Accession and End of Contract Date prior to death. Select **Next**.
7. Leave Current Home Address and Phone Numbers and Effective Date blank. Select **Finish**.
8. Add spouse to DEERS using the Add Dependent Navigator.
9. Enter Dependent’s Current Relationship, Person Identifier, Date of Birth, and any applicable Continuation Options. Select **Next**.
10. Enter Name, Gender, and Physical Attributes. Select **Next**.
11. Select any applicable Eligibility Conditions. Select **Next**.
12. Enter Current Home Address and Phone Numbers and the Effective Date. Select **Finish**.
13. On Summary, select **Create**.
14. Once the family is displayed on the Family Tree, open sponsor’s **Characteristics** view.
15. On the **Features** tab, enter Date of Death.
16. Select the Save Family  icon from the main toolbar.

**Note:** Service Record is automatically disabled. Spouse/family members keep their existing benefits. Spouse shows relationship of **Spouse (URW)** on DEERS but the DD Form 1172 and ID card will print the relationship of **URW**.

### 7.32.2 Issue ID Card to Dependent of Deceased Reserve Retired Sponsor Who Died Before 60<sup>th</sup> Birthday

1. Open Family. If sponsor does not show on DEERS, add sponsor and Reserve Retired Category as detailed in *Scenario 7.31.1*.
2. Add spouse (see *Scenario 7.3*)
3. Terminate the sponsor due to death by entered Date of Death in Characteristics view.
4. Sponsor should still show as Reserve Retired (not Retired) since he died prior to age 60.
5. Spouse (URW) should display all benefits.
6. Select the Save Family  icon from the main toolbar.

---

## 7.33 Suspended Benefits

### 7.33.1 Suspend Benefits

1. Open Family.
2. Open person's **Benefits** view.
3. On the **Suspensions** tab, click **Add Suspension**.
4. Select the Benefit(s) to be Suspended, enter Suspension Begin and End Dates, select Reason for Suspension from the drop-down list, and enter the Name of Person Initiating the Suspension. Select **Finish**. ID card can only be issued up until end of suspension.
5. On Summary, select **Create**.
6. Select the Save Family  icon from the main toolbar.

**Note:** Suspension of Direct Care should only be used as directed by Instruction from SPOs. Reasons for suspension of Direct Care (Medical) are:

- Refused to provide SSN.
- SSN not provided after grace period.

### 7.33.2 Terminate Suspended Benefits

1. Open Family.
2. Open person's **Benefits** view.
3. On the **Suspensions** tab, select the benefit you want to reinstate.

4. Click **Terminate Suspension**. Select **Separate** and enter the Date of Termination for the suspension. Select **Finish**.
5. On Summary, select **Separate**.
6. Select the Save Family  icon from the main toolbar.

**Note:** Dates for the suspension will still be displayed.

---

## 7.34 Reserve Officer Training Corps

### 7.34.1 Add a Reserve Officer Training Corps Sponsor

1. Select the **New Family** command from the **File** menu.
2. Type the Sponsor's Identifier and select **Enter**.
3. The Add Sponsor Navigator will walk the user through the steps necessary to add a new sponsor to the DEERS database.
4. Enter **Reserve** for the Sponsor's Personnel Category and any applicable Continuation Options. Select **Next**.
5. Enter Name and Marital Status. Select **Next**.
6. Enter Date of Birth, Gender, and Physical Attributes. Select **Next**.
7. Select Sponsor's Service Branch, Reserve Officer Training Corps (ROTC) for Rank, Pay Grade, and enter Eligibility Date of Accession and Date of Termination (class start date and class estimated graduation date). Select **Next**.
8. Enter Current Home Address and Phone Numbers and the Effective Date. Select **Finish**.
9. On Summary, select **Create**.
10. Continuation Options to Add Dependents, Create a DD Form 1172, or Create an ID Card are all options that will guide the user to other navigators for these additional functions.
11. Select the Save Family  icon from the main toolbar.

### 7.34.2 Terminate an ROTC Graduate Who is Awaiting Active Duty Assignment

1. Open Family.
2. Open the Service Record view.
3. On the *Branch, Rank, Pay Grade* tab, change the rank and pay grade as appropriate. Enter the date when the change will take effect. (**Note:** Destroy the ROTC Reserve card).

On the *Personnel Category* tab, correct the End of Contract date to reflect one day prior to the Sponsor's Active Duty assignment date.

4. Select the **Save Family** icon from the main tool bar, and issue the Reserve card.

### 7.34.3 Terminate a Reserve card for an ROTC Graduate Who Attains Active Duty Status the Day after Graduation

1. Open Family.
2. Open **Service Record** view.
3. On the *Personnel Category* tab, click **Terminate Personnel Category**.
4. Select **Separation**. Select **Next**.
5. Enter Date of Separation. Select **Finish**.

**Note:** Separation attributes (SPD Code, Reenlistment Code, and Character of Service) are not required to complete this operation.

6. On Summary, select **Finish**.
7. On the *Personnel Category* tab, click **Add Personnel Category**.
8. Select **Active Duty**. Select **Next**. Select **Service Branch, Rank, Pay Grade and Contract Begin and End Dates**. Current contract begin date must be at least one day after Date of Separation from ROTC. Select **Finish**.
9. On Summary, select **Create**.
10. Select the Save Family  icon from the main toolbar.

---

### 7.35 Terminate a Dependent Child that is Becoming a Sponsor

1. Open existing Family record.
2. Open the dependent's **Characteristics** view.
3. On the *Relationship* tab, click **Terminate Relationship**.
4. Select **Separation**. Select **Next**.
5. Enter **Became a Sponsor** for the Termination Reason and End Date. Select **Finish**.
6. On Summary, select **Terminate**.
7. Select the Save Family  icon from the main toolbar. Close the family.

8. Open the Dependent using his/her Identifier. Select **Yes** when prompted, “Open the family and create a Service record?”
9. Select Sponsor’s Personnel Category and any applicable Continuation Options. Select **Next**.
10. Select Sponsor’s Service Branch, Rank, and Pay Grade and enter the Eligibility Date of Accession and Date of Termination. Select **Finish**.
11. On Summary, select **Create**.
12. Select the Save Family  icon from the main toolbar.

**Note:** New sponsor must be at least 17 years old. If you are going to print a DD Form 1172 and ID card for this new sponsor, blood type and marital status must be added. Do not terminate the relationship with sponsor if family member is not immediately going on Active Duty.

---

### **7.36 Add a DoD Civil Service Sponsor and Issue the CAC**

1. Select **New Family** from the **File** menu.
2. Type the sponsor’s identifier and select **Enter**.
3. The Add Sponsor navigator will guide the VO through the steps necessary to add a new sponsor to DEERS. Select DoD Civil Service as the Personnel Category. Select **Next**.
4. Enter the sponsor’s Name and Marital status. Select **Next**.
5. Enter the Date of Birth, Gender, and physical attributes. Select **Next**.
6. Enter the sponsor’s Pay plan and Grade, Date of employment, Estimated date of retirement, Work e-mail address, and Agency/Subagency (also referred to as Service Organization). Select **Next**.
7. Enter the sponsor’s Home address, Phone number, and Home e-mail address with effective dates. Select **Finish**.
8. On Summary, select **Create**.

**Note:** Family members should not be added to DEERS unless they are receiving DoD benefits.

---

### **7.37 Add a DoD Contractor**

1. Select **New Family** from the **File** menu.
2. Type the sponsor’s identifier and select **Enter**.
3. The Add Sponsor navigator will guide the VO through the steps necessary to add a new sponsor to DEERS. Select DoD Civil Service as the Personnel Category. Select **Next**.

4. Enter the sponsor's name. Select **Next**.
5. Enter the Date of birth and Gender. Select **Next**.
6. Enter the sponsor's Pay plan and Grade, Date of employment, Estimated date of retirement, Work e-mail address, Agency/Subagency, and DoD Contract type. Select **Next**.
7. Enter the Pay category and Geneva Conventions category. Select **Next**.
8. Select **Finish**.
9. On Summary, select **Create**.

Use the following scenarios as guidance when determining a contractor's begin date for CAC issuance. In general, the start date should be the later of 1) contract begin/award or 2) date the contractor joined the contract.

1. A contractor is on staff at a CAC required company when the contract is awarded/renewed, so the CAC start date is the begin date of the new/renewed contract.
2. A contractor works for a company on a non-CAC required account then joins a CAC required contract after the award/renewal of the contract. The CAC start date would be the date the contractor joined the CAC required contract.
3. A contractor works for a company that has a CAC required contract and leaves that company. He begins work with a different company for the same CAC required contract. The sponsor would get a CAC with the first company with the contract date that applies to him in example 1 or 2 which would be terminated when he leaves the first company. A new CAC would be issued when he goes to work for the second company with the begin date being the day he started with the new company on the CAC required contract.

**Note:** Family members should not be added to DEERS unless entitled to receive DoD benefits.

---

### **7.38 Add Civil Service/DoD Contractor Personnel Category to an Existing Sponsor**

1. Open Family.
2. Open **Service Record** view.
3. On the **Personnel Category** tab, click **Add Personnel Category**.
4. Select **DoD Civil Service** or **DoD Contractor**.
5. Select Sponsor's Service Pay Plan and Grade; enter Date of Employment (for a Contractor this would be the later of the contract begin/award date or the date the contractor joined the contract) , Date of Retirement (estimated), Sponsor's Service/Organization, and DoD Contractor type if applicable.

6. Select the Save Family  icon from the main toolbar.
7. The Create ID Card Navigator will guide the user through the steps to issue the CAC.

**Notes:** The “Living in Quarters” condition allows CONUS Government civilians to have an automated ID card.

Do not issue DD Form 2765/ DD Form 1173 with a future start date.

---

### 7.39 Add a Benefit Eligible Condition to a Civil Service or DoD Contractor

Retirees working as Civil Servants or DoD/Other Government Contractors overseas are eligible for two different benefit sets. Dual Status should not be selected for the sponsor’s card; the Overseas Only stamp will automatically print on the sponsor’s CAC. The sponsor may also carry a DD Form 2 (Blue) Retired card.

1. Open Sponsor.
2. Open **Service Record** view.
3. Select a Personnel Condition from the following: **Non-CONUS Assignment, Living in Guam or Puerto Rico, Living in Quarters, Emergency Essential- Overseas Only, Emergency Essential-CONUS/Living in Quarters.**
4. Select the Save Family  icon from the main toolbar.
5. The Create ID Card Navigator will guide the user through the steps to issue the CAC.

**Notes:** The “Living in Quarters” condition allows CONUS Government civilians to have an automated ID card.

---

### 7.40 Add Emergency Essential Civilian Sponsor and Issue Geneva Convention Card

1. Select the **New Family** command from the **File** menu.
2. Type the sponsor’s identifier and select **Enter**.
3. The Add Sponsor Navigator will guide the user through the steps necessary to add a new sponsor to the DEERS database. These steps include adding the sponsor’s Personnel Category, Name, Marital Status, Date of Birth, Gender, Physical Attributes, Service Branch, Rank, Pay Grade, Eligibility Start and End Dates, Address and Phone Numbers. Continuation Options to Add Dependents, Create DD Form 1172, or Create ID Card will guide the user to other navigators for these additional functions.
4. On the Add Sponsor Navigator- Personnel Condition dialog box, select **Emergency Essential- Overseas Only** and enter the effective dates of the condition. The Effective Start and End Dates for this condition must be supported by properly signed documentation from Civilian Personnel.

5. On Summary, select **Create**.
6. Select the Save Family  icon from the main toolbar.
7. The Create ID Card Navigator will guide the user through issuing the new CAC.

**Note:** Dependents should be added as detailed in *Scenario 6.3* and issued the DD Form 1173. A Relationship Condition of “Accompanying Sponsor” must be added (if applicable) to generate benefits.

The Sponsor will surrender their current civilian ID card (DD Form 2765) to the ID card IO upon receiving their Emergency Essential Civilian ID card (CAC). Upon completion of his/her Emergency Essential assignment, the sponsor will be provided a newly signed document from Civilian Personnel to receive his/her replacement civilian ID card (CAC).

Geneva Convention Category Codes include:

- I Category I (pay grades E1 through E4)
- II Category II (pay grades E5 through E9)
- III Category III (pay grades W1 through 003 and/or Cadets and/or Midshipmen)
- IV Category IV (pay grades 004 through 006)
- V Category V (pay grades 007 through 011)
- N/A Not applicable (nonprotected personnel)

---

#### 7.41 Add Foreign Military Active Duty Member (NATO and Non-NATO) Serving in the United States Under Sponsorship of the DoD

1. Select the **New Family** command from the **File** menu.
2. In the New Family dialog box, select the FIN as the type of sponsor identifier by clicking on the arrow to the right of the SSN box. If **Open Family** is selected in error, RAPIDS will not add a new Foreign Identification Number.
3. At Add Sponsor Navigator, select Personnel Category of **Foreign Military**. You will notice that the RAPIDS system will display a FIN for the sponsor. The Add Sponsor Navigator will guide the user through the necessary steps to add a new sponsor to the DEERS database. The user should select Continuation Options for Personnel Condition, Create DD Form 1172, and Create ID Card. These navigators will guide the user through the steps for these additional functions.
4. At Foreign Military Service record, confirm citizenship or enter the **Country of Origin, Sponsor’s Service, Rank and Pay Grade**. If no rank and pay grade is available, select **Other**.
5. If **Other** was selected, enter the Sponsor’s Pay Category.

6. At Personnel Condition dialog box, select **DoD Sponsored in US** and enter the Effective dates for this condition.
7. On Summary, select **Create**.
8. Select the Save Family  icon from the main toolbar.
9. Selected navigators will guide the user through creating the DD Form 1172 and/or ID Card.

**Note:** Dependents should be added as detailed in *Scenario 7.2* using the FIN or SSN as the type of identifier and issued the DD Form 1173. A check mark should never be placed in the None box. A Relationship Condition of “Accompanying Sponsor” must be added (if applicable) to generate benefits.

Refer to the Interservice Publication for the differences in benefits for NATO and Non-NATO personnel and their dependents.

Some NATO sponsors may have identifiers beginning with 915 or 800. Please disregard these identifiers for this system. A new 900 series FIN should be generated for those sponsors.

---

## 7.42 Transitional Compensation for Abused Family Member

### 7.42.1 Update a Family Member Entitled to Transitional Compensation Due to Abuse (Sponsor on Active Duty Over 30 Days or Retirement Eligible)

Contact your PO in all cases of dependent abuse as they can advise on whether the dependents meet the eligibility criteria. The PO will update DEERS and assist VOs in preparing the DD Form 1172 for issuance of ID cards. The DD Form 2698, *DD Form 2698 Application For Transitional Compensation* should be forwarded to the PO to ensure that the sponsor’s and family members’ RAPIDS records correctly reflect their ID card entitlements.

Once the sponsor’s record is modified to reflect dependent abuse, the sponsor will no longer display the Benefits view.

Former Spouse Qualification screen must be completed regardless of marital status. Children are eligible for benefits until the age of 18 unless incapacitated or full-time student status. **Note:** The ID card will display the sponsor's rank and pay grade prior to any demotions.

Once the eligibility criteria have been determined, [refer to the Interservice Publication AFI 36-3026], the following scenario can be completed. **Note:** This scenario can be used for eligible family members (unmarried child, adopted child, stepchild who resides with the sponsor at the time of abuse, spouse, and former spouse) entitled to Transitional benefits due to abuse.

The Sponsor must have met the following criteria.

- Retirement eligible and eligibility to retired pay is terminated.
- On Active Duty over 30 days (who is separated due to misconduct).

- Separated under a court-martial sentence resulting from family abuse offense.
  - Administratively separated on the basis of family abuse offense.
  - Sentenced with forfeiture of all pay and allowances by a court martial.
1. Open Sponsor's record that is either on Active Duty for more than 30 days or retirement eligible.
  2. Verify Active Duty sponsor's personnel conditions, so that the sponsor's service record(s) reflect Appellate Leave or Military Prisoner.
  3. Verify sponsor's record (who is on AD or Ret eligible) under personnel category, so that the sponsor's separation attributes and date (due to administrative action or court martial) is listed.
  4. Open the affected family member's **Characteristics** view  icon, and select **Relationship Condition**, and then select either **Transitional Compensation on AD** or **Transitional Compensation for Ret**. The following description will read "Effective date of removal," this is the effective Start date of payment as listed on *DD Form 2698 Application For Transitional Compensation*, under Block 21a. The following description will also read "Date family member entitlement ended," this is the Stop date of payment as listed under Block 21b. **Note:** For family members whose sponsor is retirement eligible, enter the effective Start date and termination Stop date as reflected on the memorandum from the Defense Finance and Accounting Service or finance office or select the "Unknown" box for indefinite periods.  
**Note:** The description will read as follows. "Transitional Compensation on Active Duty, sponsor is ineligible for retirement; and Transitional Compensation for Retirement, sponsor is eligible for retirement."  
**Note:** For family members whose sponsor is retirement eligible, enter the effective Start date and termination Stop date as reflected on the memorandum from the Defense Finance and Accounting Service or finance office or select the "Unknown" box for indefinite periods.
  5. Select **Finish**.
  6. Select **Save**.

#### 7.42.2 Divorce a Spouse Who is Eligible for Transitional Compensation from a Sponsor, Due to Family Abuse

1. Open Family.
2. Open Spouse's **Characteristics** view  icon.
3. On the **Relationship** tab, select **Terminate Relationship**.
4. Select **Separation**, then **Next**.
5. Select **Divorce Due To Family Abuse**, and enter **Final Divorce Decree Date**; select **Next**.

6. Complete the Former Spouse Qualification attributes with the following conditions: (1) Enter the number of years of marriage; (2) the sponsor's length of service; and (3) the number of years of marriage that overlaps with the sponsor's years of service. Finally, select the **Eligible for Transition Compensation** box.
7. Select **Finish**.
8. On Summary, select **Terminate**.  
**Note:** The description should read "Former Spouse as a result of an Abused Relationship." ID card benefits should not disappear!
9. Select the Save Family  icon from the main toolbar.

---

### 7.43 Add Former Member

1. Select **File|New Family**.
2. Type the Sponsor's Identifier, and select **Enter**.
3. The Add Sponsor Navigator will guide the user through the steps necessary to add a new sponsor to the DEERS database. Enter Sponsor's Personnel Category (Former Member) and any applicable Continuation Options. Select **Next**.
4. Enter Name and Marital Status. Select **Next**.
5. Enter Date of Birth, Gender, and Physical Attributes. Select **Next**.
6. Select Sponsor's Service Branch, Rank, Pay Grade, and enter Eligibility Date of Accession. Leave the field blank for Date Granted Pay. The card will print with the expiration date of four years. Select **Next**.
7. Enter Current Home Address and Phone Numbers and the Effective Date. Select **Finish**.
8. On Summary, select **Create**.  
**Note:** When the sponsor applies and is granted pay (often at age 60), the Former Member category can be terminated, and a Retired category can be added.

---

### 7.44 Create Temporary ID Card

A temporary ID card may need to be issued if a user is awaiting documentation or the Sponsor's signature. Temporary ID cards are any ID cards with an expiration date less than the system generates.

1. Open Sponsor.
2. Open **Characteristics** view for the dependent to update, and complete hair and weight information.

3. Select the Save Family  icon from the main toolbar.
4. Select **Create DD Form 1172 Navigator**.
5. On the Create DD Form 1172 Navigator – Select Form screen, select the appropriate Sponsor Category/Condition. Select **Next**.
6. Select the dependent that is to receive the temporary card. Highlight the card expiration date found on the far right side of the screen, and change it to reflect the correct date. Select **Next**.
7. On the Create DD Form 1172 Navigator – ID Card Expiration Date Change Reason screen, select the ID card Expiration Date Reason from the drop-down list. Select **Next**.
8. On Summary, select **Next**.
9. Print the DD Form 1172.
10. Select the Create ID Card Navigator, and check the expiration date of the ID card on the navigator screen. If the date is correct, produce the ID card.

**Note:** The Family Tree will display an icon to indicate that a temporary ID card was issued. The ID Card person view will state “Temporary” in the lower right-hand corner.

---

#### 7.45 Adding/Updating E-mail Certificates on an Existing CAC

1. Open Family.
2. Open Service Record.
3. At the **Personnel Category** tab, enter the Work E-mail Address.
4. Select “Update CAC “ function by either right clicking on the icon for the sponsor’s existing CAC -or- highlighting the existing CAC icon and selecting the “Update CAC” button from the RAPIDS tool bar.
5. The Progress Meter will display as the chip is updated.

---

#### 7.46 Create DD Form 1172 and ID Card

To create a DD Form 1172 and an ID card for the above scenarios, first SAVE the updated family. If the user forgets, RAPIDS will prompt the user to save any changes to DEERS.

##### 7.46.1 DD Form 1172

1. Select **Beneficiary** or **Family** from the main menu and **Create DD Form 1172** from the drop-down list.  
-or-

Select the Create DD Form 1172 icon from the main toolbar.

2. The DD Form 1172 Navigator will guide the user through the steps of selecting the Sponsor's personnel category, condition, and family members, entering remarks, VO information, IO information, and printing the form.

#### **7.46.2 ID Card**

1. Select **Beneficiary** or **Family** from the main menu and **Create ID Card** from the drop-down list.

-or-

Select the Create ID Card icon from the main toolbar.

2. The ID Card Navigator will guide the user through selecting an ID card to capture, print, and accept the photograph.
3. The system will instruct the user on the type of cardstock to place in the printer and guide the user through printing the front and back of the ID card.

If your site has a Hewlett Packard (HP) LaserJet 6P printer, it is essential that the teslin cardstock be aligned correctly in the manual feed chute. If the cardstock is not aligned properly, it may jam; to avoid this scenario, adhere to the following guidelines.

4. Do not pull the cardstock through the rollers. Allow the cardstock to feed through the printer at its own pace.
5. Wait approximately 15 seconds before feeding the cardstock back into the printer to print the back of the ID card. This allows the cardstock to cool sufficiently, thus reducing the occurrence of jams.

#### **7.46.3 Laminate the Teslin ID Card**

1. Power the laminator on, and check that the heat level is within the accepted (green) range.
2. Ensure that the card recipient has signed the teslin ID card.

**Note:** The CAC is automatically laminated by the printer. Do not attempt to laminate the CAC using this procedure.

3. Insert the ID card into the laminate with the top of the card closest to the fold of the laminate. The hologram should display on the front side of the card.
4. Ensure that the cardstock is completely centered in the laminate.
5. Insert the card lengthwise into the laminator, and switch the laminator to the run mode. Do not use cardboard to protect the ID card.

## 8 Using RAPIDS SVO Functions

RAPIDS offers additional tools for use by the SVO. This section will explain these tools and identify the different reports available with the RAPIDS application.

---

### 8.1 SVO Functions and Descriptions

SVO functions consist of all VO duties as well as specialized duties, such as managing all report functions. RAPIDS transactions are recorded for use in reports. Only the SVO for a specific site will have access to the reports options under **Tools**.

---

### 8.2 Site Information

Address data that pertains to your specific site and is used in producing the DD Form 1172 can be updated by the site's SVO.

1. Select **Tools** from the main menu bar.
2. Select **Site Address** from the drop-down list.
3. At Site Information, click **Modify Site Info** to modify the site, address, and UIC information. To ensure consistency and accuracy of site information, all RAPIDS site name, city and state requests must be routed through the DEERS/RAPIDS SPO for update into a centralized database. See *Appendix C* to determine the SPO for your site.
4. Click **Commit** to save changes.

---

### 8.3 Remarks

Remark data that is used in producing the DD Form 1172 is stored by site ID at the server. The system will have certain predefined remarks. The SVO can view, update, delete, and add remarks in the listing for assigned site(s). Use the following steps to add a new remark.

1. Select **Tools** from the main menu bar.
2. Select **DD Form 1172** from the drop-down list.
3. At the Remarks window, select **New...** to add a new Remark.
4. Type in the new remark desired.
5. Select **OK** to save the new remark.

**Note:** Users can only update and delete remarks that the site has previously added. Predefined remarks cannot be updated or deleted.

## 8.4 RAPIDS Reports

There are four main reports that the RAPIDS SVO may produce: (1) Error, (2) ID Card, (3) Periodic Summary, and (4) Transaction. If a security relevant report is required, it will be produced using one of the four reports.

The four reports have an initial criteria dialog box that must be completed. The initial criteria dialog box allows the reports to be previewed. Additionally, the transaction type can be specified (online, offline, or both). Advanced criteria boxes, when selected from the initial criteria dialog boxes, limit the database search and are optional.

The SVO produces customized reports by selecting and entering data through dialog boxes, drop-down lists, and options. The user can perform the following actions with reports.

1. **Print:** this displays a report on the screen (Print Preview) and prints the report on paper. To print a hard copy, select the **Output directly to printer** checkbox.
2. **Advanced:** limits the database search to create a customized report.
3. **Sort/Group:** allows the SVO to sort data by one or more items and select the grouping of data.
4. **Save:** allows the SVO to save selected report criteria.
5. **Open:** allows the SVO to open a previously saved report.
6. **Help:** provides information on generating reports.

### 8.4.1 How to Access Reports

To access reports on RAPIDS, select **Tools** from the main menu. The drop-down list under Tools contains a list of reports. Once the desired report is selected, the specific dialog boxes for that report will be displayed.

The Services have not mandated frequency, type, or selection of reports to be produced by each site. The RAPIDS application is designed to allow the SVO to custom fit report processing as each site desires. Many sites print the ID Card Report and the Transaction Report on a daily basis. The site SVO should determine the schedule for generating these useful reports.

### 8.4.2 Error Report

This report lists error codes determined by the DEERS mainframe. This report is monitored electronically by DEERS personnel who will monitor and resubmit records with offline errors. Please report any errors in the offline process to the D/RAC / D/RSC-E / DSO-A (*Appendix A* of this guide).

1. Select **Tools** from the main menu.

2. Select **Error Report** from the drop-down list to display the Error Report Criteria dialog box.
3. Type the beginning and ending dates for the report.
4. Select **site ID** and **Verifying Official(s)** as needed.
5. The **Advanced** tab allows other properties to be selected, such as Characteristics, Service Record, and Other.
6. The **Sort/Group** tab allows reports to be grouped by various criteria and sorted under that group heading.
7. Click **Print** to view and/or print the report.

**Note:** If the SVO does not wish to preview the report prior to printing, simply select the box to output directly to the printer.

If no errors exist, the VO will receive a message stating the same.



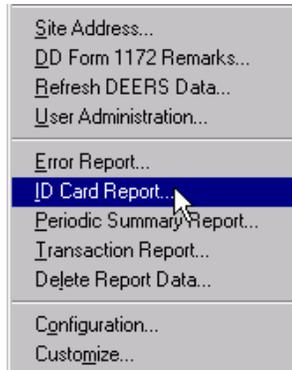
### 8.4.3 ID Card Report

This report lists the ID cards produced and can be customized.

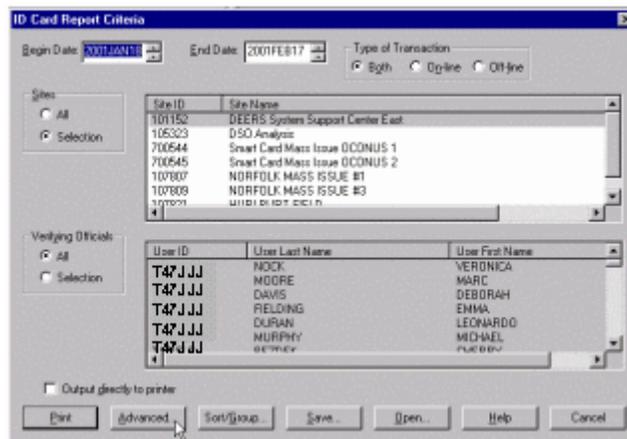
1. Select **Tools** from the main menu.
2. Select **ID Card Report** from the drop-down list to display the ID Card Report Criteria dialog box.
3. Type the beginning and ending dates for the report.
4. Select **Transaction Kind**, **site ID**, and **Verifying Official(s)** as needed.
5. The **Advanced** tab allows other properties to be selected, such as Characteristics, Service Record, and Other.
6. The **Sort/Group** tab allows reports to be grouped by various criteria and sorted under that group heading.
7. Click **Print** to view and/or print the report.

To customize a report to detail CAC issuance, use the following procedure.

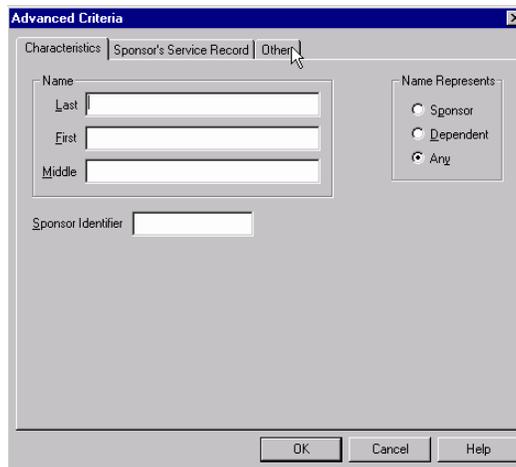
1. Select the **ID Card Report** from the **Tools** Menu.



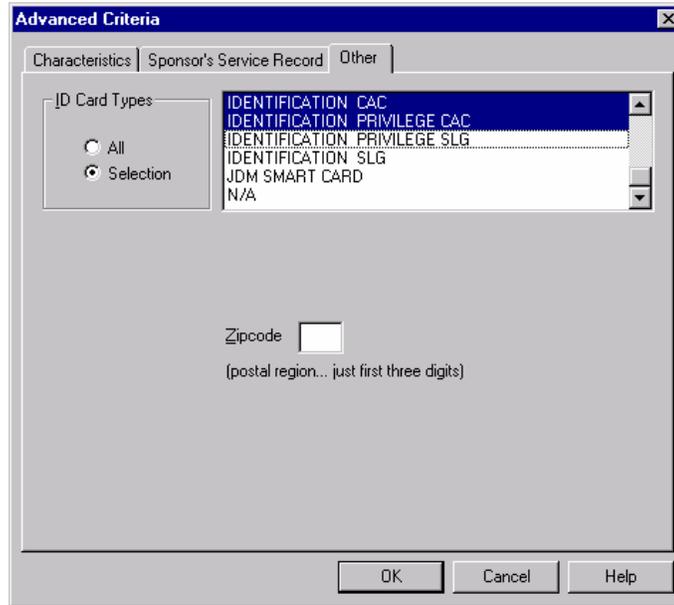
2. Click on **Advanced** to select the Card Type to report on.



3. Select the **Other** Tab.



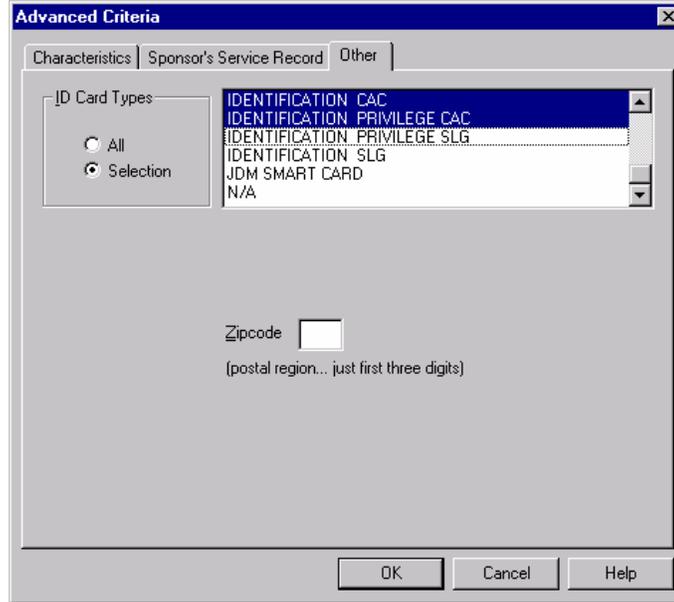
- From the **Other** tab of the Advanced Criteria, select the **Selection** radio button, then choose the appropriate option (CAC or teslin) from the list.



CAC options include:

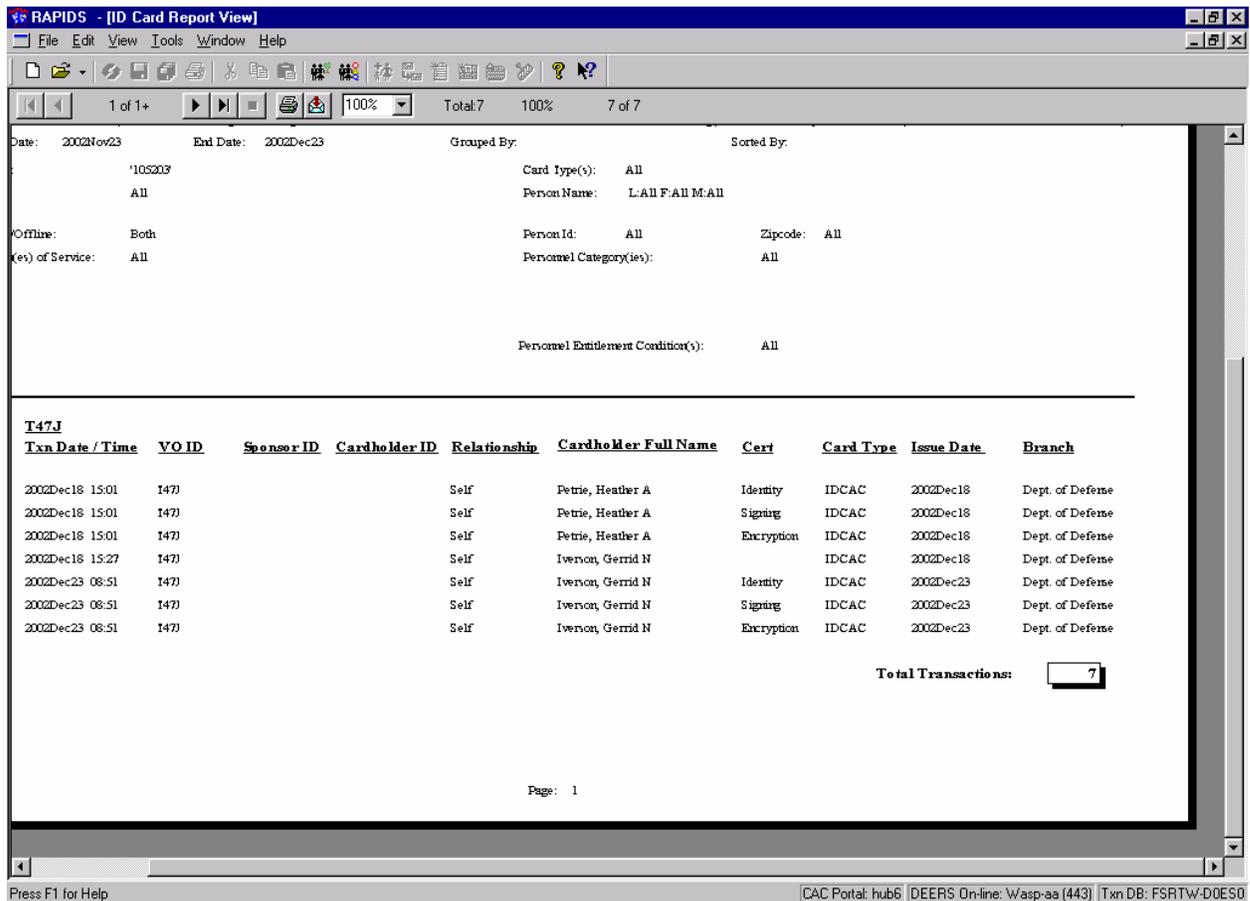
TYPE OF CARD	DEFINITION
USCAC	DoD Armed Forces CAC
IDCAC	Identification CAC for DoD Civilian employees, DoD contractors, Non-appropriated Fund employees, Foreign Nationals
IPCAC	Identification Privilege CAC for DoD contractor, DoD civilian, Foreign Military, SES, Presidential Appointee, Non-Appropriated Fund employee (all of these sponsors must have a personnel condition to get this card (other than one of the emergency essential conditions))
CGCCAC	Accompanying Armed Forces CAC for DoD contractor, DoD civilian, Foreign National, Presidential Appointee operating in an emergency essential capacity
SLG	Each type of CAC above has a non-chip card as well.

The listing of ID card types also includes the non-ICC identified with the suffix SLG for all four CAC types.



When complete, click on the **OK** button. The report will be generated. Print the report.

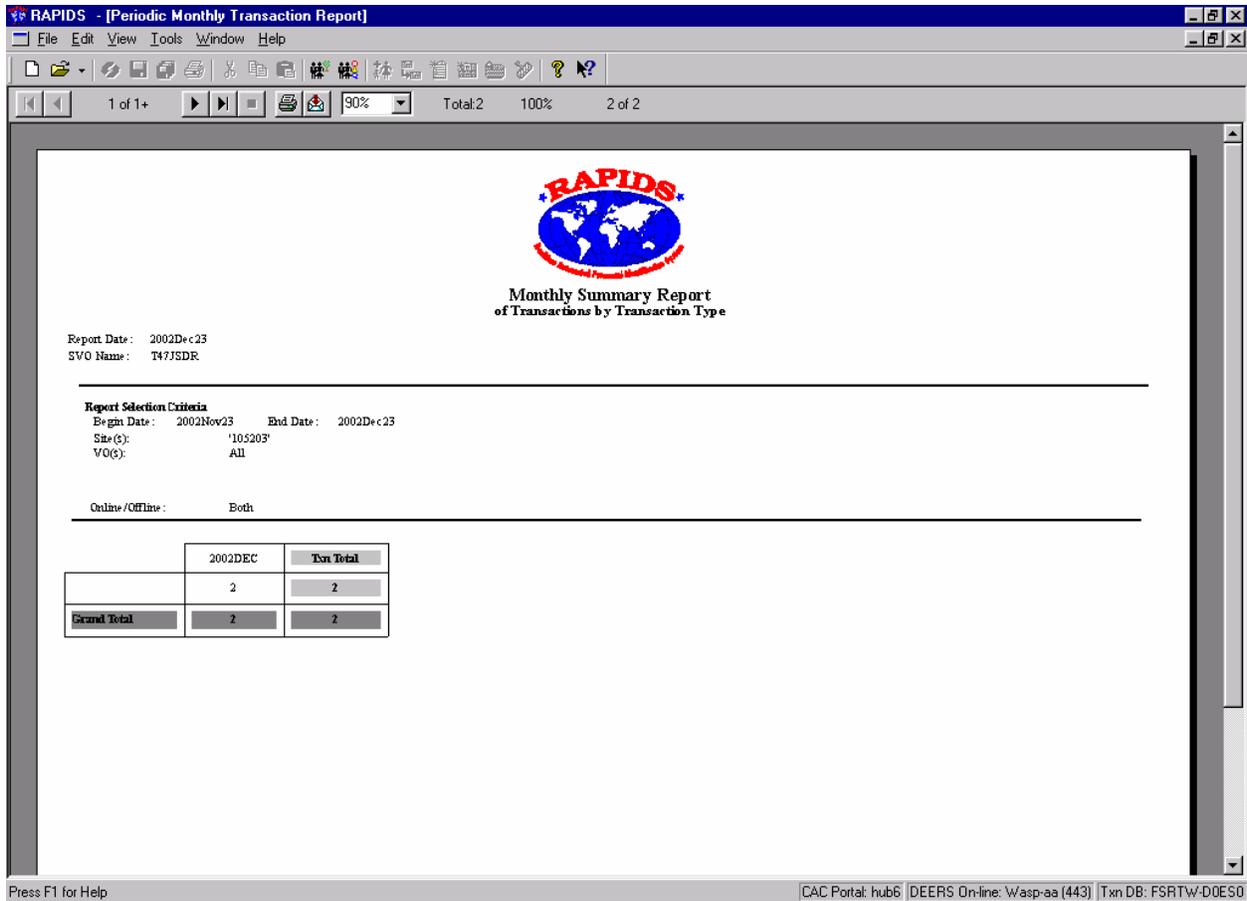
The ID card report displays the status of each certificate generated and issued.



### 8.4.4 Periodic Summary Report

This report summarizes transactions and is subtotaled by days or months.

1. From the main menu, select **Tools|Periodic Summary Report** to display the Periodic Report Criteria dialog box.
2. Type the beginning and ending dates for the report.
3. Select **Transaction Kind**, **site ID**, and **Verifying Official(s)** as needed.
4. The *Advanced* tab allows other properties to be selected, such as monthly or daily periodic format or totals.
5. Click **Print** to view and/or print the report.

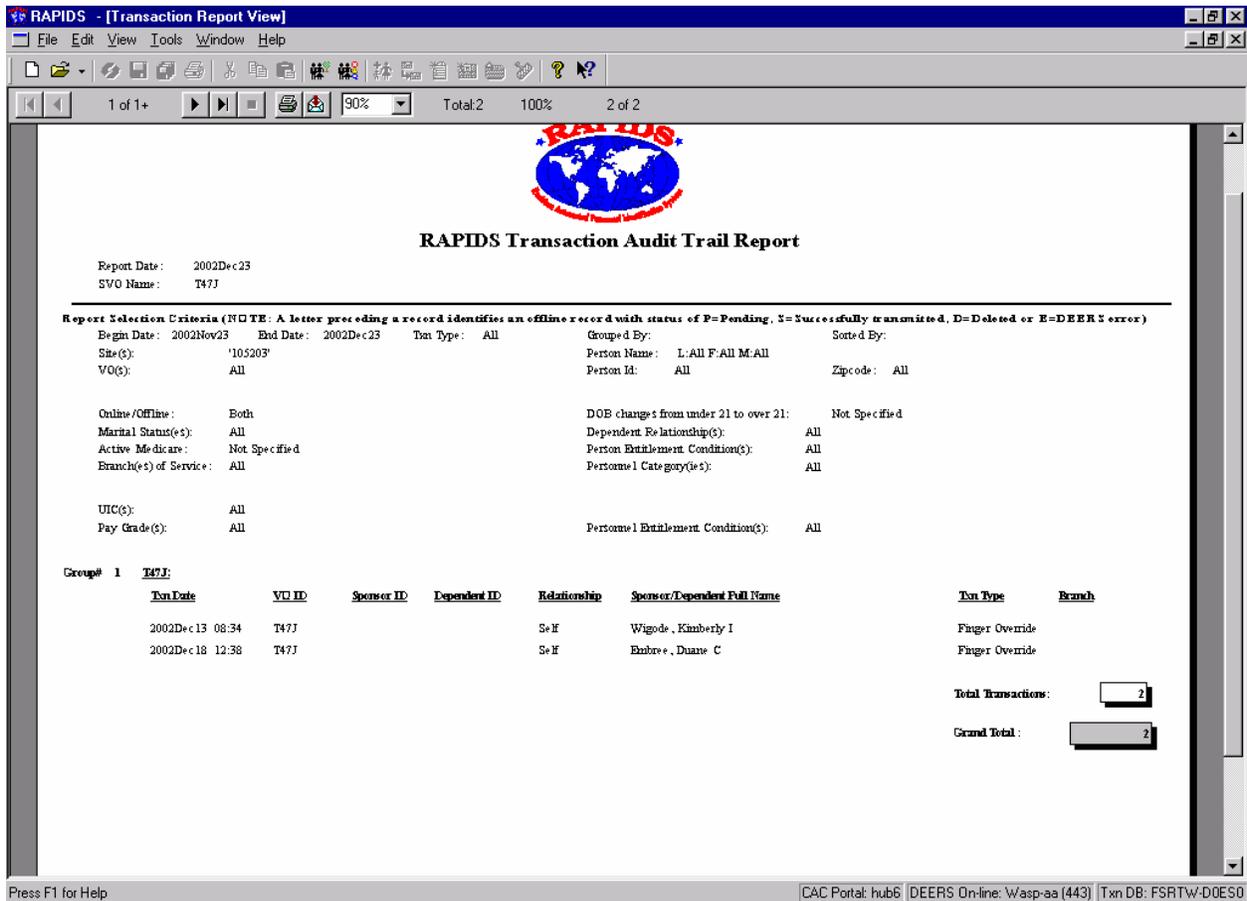


### 8.4.5 Transaction Report

This report lists the transactions performed using a RAPIDS workstation.

1. From the main menu, select **Tools|Transaction Report** to display the Transaction Report Criteria dialog box.

2. Type the beginning and ending dates for the report.
3. Select **Transaction Kind**, **site ID**, and **Verifying Official(s)** as needed.
4. The *Advanced* tab allows other properties to be selected such as Characteristics, Service Record, and Other.
5. The *Sort/Group* tab allows reports to be grouped by various criteria and sorted under that group heading.
6. Click **Print** to view and/or print the report.



### 8.4.6 Exporting Reports

This option is available from the Print Preview screen and is as simple to use as saving a document in a word processor. The Export  icon is displayed on the **Report** view toolbar. This option allows the SVO to save reports in other formats. There are many different formats to which reports can be exported. These include, but are not limited to, Microsoft Word for Windows, Microsoft Excel, LOTUS, Text (.txt) and Rich Text Format (.rtf).

1. Select **Tools** from the main menu.

2. Select the report to archive.
3. Click **Print**.
4. At the Print Preview, click **Export**  from the main toolbar.
5. In the Export dialog box, select the format from the drop-down list. Text format allows the SVO to view the report using any text editor such as Microsoft Notepad. Select the Disk file as the destination.
6. Click **OK**.
7. At the Choose Export File dialog box, select the location to save your file (e.g., 3 1/2" Floppy A:) and name your file. Click **Save**.

**Note:** If you receive an error that the drive you have chosen is not accessible in the Choose Export File dialog box, check to see if your diskette needs to be formatted.

#### 8.4.7 Deletion of Report Data

The SVOs at the server site and remote sites have the ability to delete audit trail report data from the SVO's own site ID. This function is not limited to the server site. The option to Delete Report Data is available from the SVO's **Tools** menu and is only accessible by an SVO. The user is able to choose either a range of dates in which to delete data or delete all data before a specific date. This capability allows a RAPIDS site the flexibility to delete audit (report) data to free disk space on the RAPIDS server.

The SVO at the server and remote sites will be able to delete data that is over 90 days old. There are two options for deleting this information.

1. Delete all data before a specific date.
2. Delete all data within a specific date range.

. SSM/SVOs are reminded to generate RAPIDS reports and delete Report data from the RAPIDS server when the data is no longer needed. DEERS/RAPIDS Operations Division suggests the SVO/SSM run these reports at least monthly and delete the data that is over 90 days old. Failure to delete report data can cause the RAPIDS server to run out of memory, which will disable all workstations attached to the RAPIDS server. Storing large quantities of report data can severely impact processing speed. For assistance in printing and deleting reports, contact your FSR or the D/RAC / D/RSC-E / DSO-A as listed in *Appendix A* or *B*.

## 9 Using RAPIDS SSM Functions

---

### 9.1 SSM's Security Responsibilities

Each RAPIDS site is requested to have a maximum of two (primary and backup) but a minimum of one SSM(s). Each SSM has an official need-to-know for all the information to which he/she is to have access. Local SSMs are responsible for managing the security of RAPIDS workstation(s) and server(s) that are deemed as being under his/her purview. Specific responsibilities for the SSM include:

- Act as the primary site POC for RAPIDS-related matters.
- Maintain the Site Roster of RAPIDS users. Add and assign roles for the various categories of RAPIDS users. Request a new DEERS logon ID for a new user, delete a DEERS logon ID, reset Users' passwords, update the security privileges on a previously issued DEERS logon ID. Deactivate and report security violators.
- Monitor usage of RAPIDS equipment to detect unauthorized activities.
- Report SSM changes immediately to DEERS Security.
- Maintain the Site Information (i.e., site name, site location address, site phone number(s), and site mailing address) View or update the RAPIDS configuration utilities when needed. The SSM acts as the site POC for RAPIDS-related matters.
- Be accountable for all CAC-related stock items, including CAC cardstock, non-ICC cardstock, and printer consumables.
  - To preserve accountability for CAC cardstock, the SSM must follow the prescribed Issuance Logistic Portal acceptance procedures to include signing for, verifying card numbers in the carton, and accepting/rejecting each carton of a CAC shipment before the Issuance Portal can issue CACs from that carton.
  - To preserve accountability for CAC cardstock, return "bad" (defective, incomplete, misprinted, and/or improperly functioning) cardstock following the prescribed procedures.
  - Coordinate the destruction of printer ribbons as they contain "Privacy Act" data.

---

### 9.2 User Administration

The SSM is responsible for activating all RAPIDS users and assigning roles for new and existing users. The SSM is also responsible for requesting a log on ID for a new user via User Administration and ensuring that new CACs are updated with LRA privileges. LRA privileges allow a VO a higher level of security needed to generate other CAC recipient certificates. Because of the nature of the position, an SSM must be familiar with the RAPIDS application and infrastructure, ActivCard Gold utility and RAPIDS support teams as described in *Appendix A* of

this training guide.

To be a RAPIDS CAC user, the first step is to ensure that the potential users have been issued a CAC. The identity certificate on the CAC is used to authenticate the RAPIDS user to DEERS. It may be necessary to add the new VO as a sponsor via RAPIDS to issue his/her CAC. If a new VO already has a CAC in his/her possession, it is not necessary to issue a new CAC. Continue with the process in step two.

Ensure that each RAPIDS user has a DEERS user ID. The SSM should add new users by using the New User option under **Tools|User Administration**. Existing RAPIDS users who previously accessed older versions of RAPIDS will need to be activated, then updated via **Tools|Administration** and the proper roles assigned. It may not be necessary to activate users who were using previous RAPIDS versions; however ALL users will need to have LRA privileges requested through the Certificate Authority.

To use the RAPIDS application that accesses the DEERS database, the VO must insert his/her CAC into the VO card reader. When the log on screen appears, the VO must type the PIN associated with his/her CAC in the ActivCard Gold log on screen to access Windows NT. When RAPIDS is started, the CAC and Windows NT log on information is compared to the log on ID and password stored on the server's local database to verify the user is authorized to run RAPIDS. This stored log on ID and password is also compared to information stored on the DEERS database to verify the user is authorized to access DEERS.

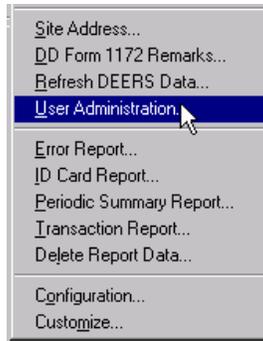
The password needed to access the RAPIDS application is the user's personal password or NT password. For security purposes, neither the password nor the PIN should be shared with anyone, including other VOs, the SVO, or the SSM. For additional system protection, neither the logon ID, password nor PIN is saved on the log on screen. The PIN will not be displayed on the screen as it is typed, instead it will be masked with asterisks “\*”.

As part of the log on procedure, the RAPIDS application prompts the VO for his/her fingerprint. As with all RAPIDS fingerprints, the right index finger should be placed on the fingerprint platen for verification. (Refer to *Section 6.1.8* of this training guide for details on the fingerprint capture process). Upon completion of the fingerprint verification, the VO is prompted to enter the six to eight digit CAC PIN.

### 9.2.1 Add New User with LRA Privileges

The RAPIDS SSM should follow these steps to add a new DEERS/RAPIDS user. The RAPIDS Installer or FSR must use this step to update an existing SSM with LRA privileges.

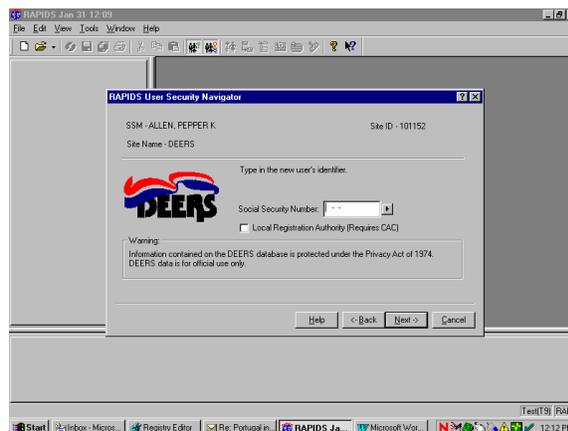
1. Select **Tools|User Administration** from the main menu.



- At the RAPIDS User Security Navigator, select **New User** and click **Next**. This action associates a new or existing DEERS user to this site. A DEERS user account will only be created if one does not exist.

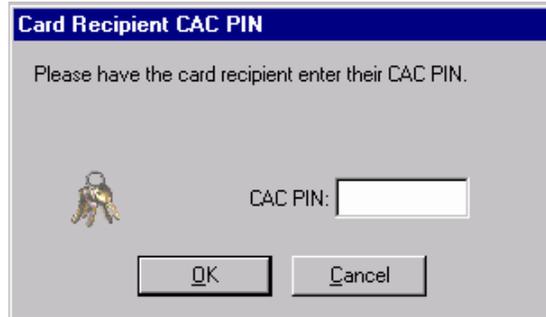


- The SSM logged into RAPIDS must have his/her CAC in the VO reader/encoder. Insert the new user's CAC into the card recipient's reader/encoder and check the box for "Local Registration Authority (Requires CAC)."

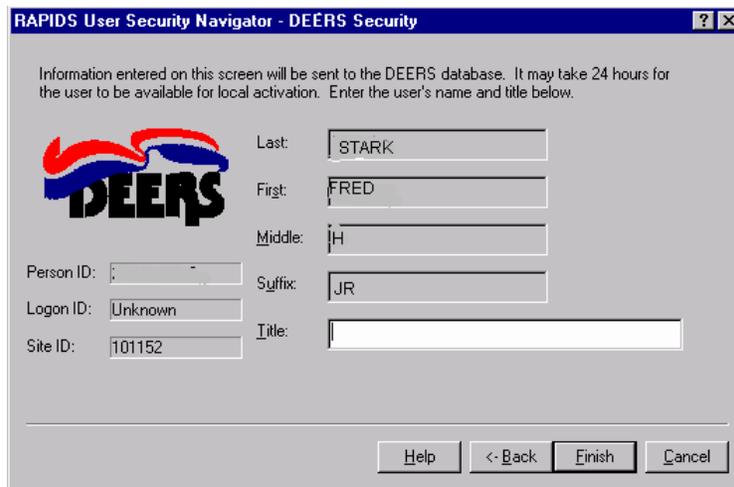


- It is not necessary to input the Person Identifier if the CAC is inserted as RAPIDS will read that information from the CAC. If prompted, the new VO should enter his/her CAC

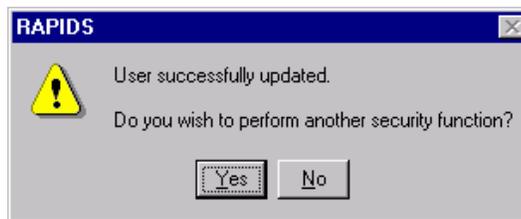
PIN (six to eight digits).



5. If the VO is already an existing VO, DEERS will return a message stating the same.
6. DEERS will return the DEERS Security dialog box. Enter or confirm the information requested. Select **Finish**.



A progress monitor will appear with a status detailing that DEERS is being updated. This action sends the update to DEERS. A confirmation message of "User Successfully Added/Updated" should appear confirming that the update was sent to DEERS. If the confirmation message does not appear, the LRA privileges may not have been successfully updated.



The VO's request to be added to the LRA security table will process within 48 hours. After the 48 hour request period, the new VO will be able to conduct RAPIDS user functions on a RAPIDS version 6 workstation. The newly updated RAPIDS user will not be able to log on to RAPIDS using his/her CAC until the following business day.

Issuing a CAC to an individual that is a VO does not enable them to perform VO functions under a RAPIDS version 6 workstation. After the VO is updated, following the steps listed, the VO must then register their CAC on each RAPIDS version 6 workstation and set their Windows NT Login Account for the RAPIDS version 6 server. Follow the procedures detailed in *Section 5.3.2* of this training guide.

The log on ID and initial password will be generated overnight for new users. A form will be mailed to the newly added user with the new log on ID and password. After the new user receives their DEERS ID and initial password, the RAPIDS SSM should activate the user and assign the appropriate roles for the new user. If the new user has been created to serve as the primary or secondary SSM, the current SSM must contact the security section of the D/RAC to have the user added as an SSM for that site. Once the user is updated in DEERS as an SSM, he/she must be updated through User Administration for the SSM role.

### 9.2.2 Activate User and Assign Roles

RAPIDS users may have more than one role at any given time (for example; VO, IO, SVO, and SSM). Users with multiple roles will not have to logoff and log on again in order to switch between roles. The RAPIDS SSM should follow these steps to activate a new DEERS/RAPIDS user and assign roles, once they receive their log on ID and initial password from the DEERS Security Office. The Activate User option does not request LRA privileges from the CA.

1. Select **Tools|User Administration** from the main menu.
2. At the RAPIDS User Security Navigator, select **Activate User** and click **Next**.
3. Select the user you wish to activate, and click **Next**.
4. Input the pay grade and phone number, and enter the DEERS password. Click the desired role in the Available box and click >>. The role appears in the Assigned box. (Multiple roles can be selected).
5. Select **Finish**.

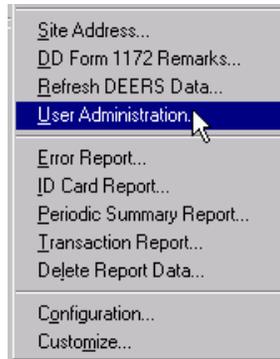
**Note:** The Update User Screen can be customized to list users alphabetically, by DEERS ID, or by SSN. Simply select the column name that you which to sort by.

### 9.2.3 Update User Information (Update LRA Privileges, Update Name, Phone Number, Pay Grade, Title Roles)

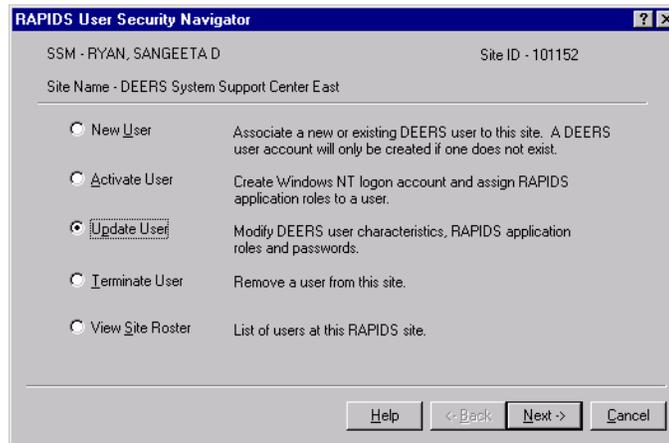
SSMs who are updating an existing RAPIDS user to have LRA privileges should use this function. This same procedure must be followed when a new CAC is issued to any RAPIDS user. In the cases of a new CAC being issued to an existing VO, the VO must wait 48 hours after being updated on the LRA table to resume CAC related VO responsibilities. Because of this, the SSM must plan ahead when a current RAPIDS user is scheduled to receive a new CAC (promotion, name change, etc.).

If a new CAC is issued or if information changes on a VO, these processes need to be repeated with the newly issued CAC.

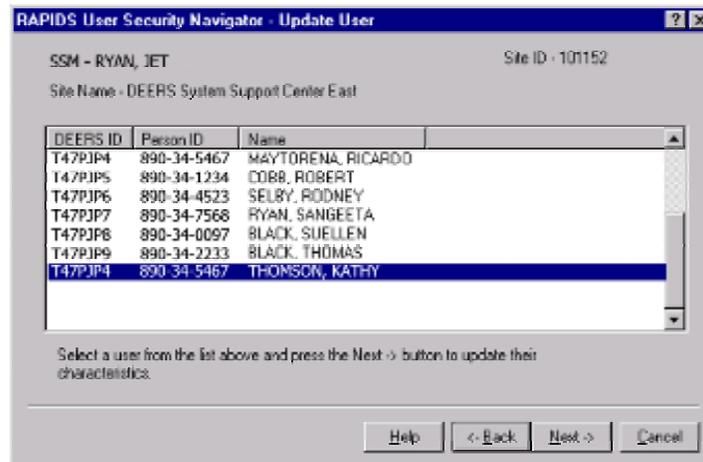
1. Select **Tools>User Administration** from the main menu.



2. At the RAPIDS User Security Navigator, select Update User and click Next.

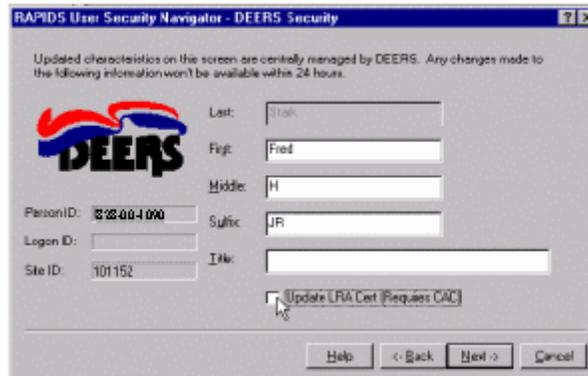


3. Select the user for which you wish add LRA privileges or update.



4. Insert the CAC for the VO you wish to update into the card recipient reader/encoder.

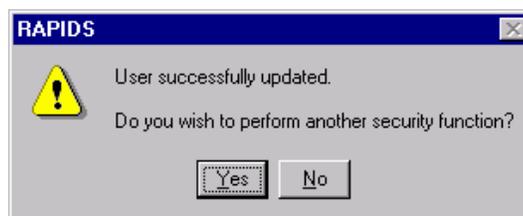
5. Check the box for “Update LRA Cert (Requires CAC)” to ensure that the LRA privileges are added. This privilege allows a VO to use his/her CAC to create other CACs.



6. The VO being updated will be prompted to enter their PIN.



7. When prompted, update the pay grade and phone number. Click the desired role in the Available box and click >>. The role appears in the Assigned box. (Multiple roles can be selected). Select **Finish**. This action sends the update to DEERS. A confirmation message of “DEERS user characteristics successfully updated” should appear confirming that the update was sent to DEERS. Select **NO** to finish.



**Note:** If after the 48 hour period, the VO experiences problems logging on to RAPIDS, call the D/RAC to ensure that the VO is set up on the Sign on Table.

## 9.2.4 Terminate Users

The SSM must closely manage the site’s RAPIDS user base. If a DEERS/RAPIDS user is being reassigned or no longer needs access to DEERS/RAPIDS, then he/she must be terminated by the

RAPIDS SSM. The SSM should follow these steps to terminate a DEERS/RAPIDS user.

1. Select **Tools|User Administration** from the main menu.
2. At the RAPIDS User Security Navigator, select **Terminate User**.
3. Select **User ID** to be terminated.
4. Select **Finish**.

### 9.2.5 View Site Roster

Regularly a RAPIDS SSM will need to review the list of DEERS/RAPIDS users at his/her site. The Site Roster provides the SSM with an additional tool to better monitor and administer the site's RAPIDS user base. The SSM should follow these steps to view all active DEERS/RAPIDS users.

1. Select **Tools|User Administration** from the main menu.
2. At the RAPIDS User Security Navigator, select **View Site Roster**.
3. Select **Finish**.

---

## 9.3 CAC stock and consumables

CAC stock and Fargo ProL printer related consumables are not ordered through the same channels that current teslin card stock, laminate and toner cartridges are supplied through. A secure Web-based automated card management system has been developed to ensure accountability of CAC stock and automate the ordering process. All CAC stock ordering will be managed by this system based on the site's stock levels, card issuance rates and an assigned reorder threshold. The SSM will be responsible for logging onto this system to account for CAC stock shipments received and to account for expired, collected or defective CACs. If the SSM has not logged on and accounted for each box of CAC stock received, the site will not be able to use that CAC stock until the SSM activates that box through the automated card management system.

---

## 9.4 Policy and procedure compliance

A SSM has the responsibility to manage site policies and procedures. These policies include all security policies detailed in this training guide as well as those outlined in the RAPIDS Security Standard Operating Procedures (SOP). Additionally, the SSM is typically the site's authority on ID card and benefits policies as defined in the Interservice publication. The SSM must also be aware of the various procedures for maintaining a secure and productive site. One key procedure involves the coordination of the SSM position to account for SSM attrition.

With the addition of the CAC to the log on procedure, the SSM must arrange that an overlap period exists between the out-processing and in-processing RAPIDS SSM. The out-processing

SSM must issue a CAC to the in-processing SSM and add him/her as a new user through the **Tools|User Administration** function of the RAPIDS software. This will require inserting the new SSM's CAC into the card recipient's smart card reader/encoder and adding the new SSM to the LRA table. If the new SSM is currently a VO at the site, then a new CAC will not have to be created. Prior to his/her departure, the out-processing SSM should coordinate with DEERS/RAPIDS Assistance Center's Security Team to ensure that the new SSM has been granted the SSM role and has been added. This role cannot be added without the assistance of DEERS/RAPIDS security personnel.

Please note that the assignment of an SSM is a manual process and can take as long as 48 hours to be effective. If no overlap occurs between the SSM, another VO can issue a CAC to the new SSM, but will be unable to add the new SSM to the LRA table. In these cases, coordination with the DEERS/RAPIDS security personnel to add the SSM to the LRA table and assign the SSM role as required. Exception: If the new SSM is already a VO for the site, the current SSM must contact the security section of the D/RAC to have the user added as an SSM for that site. Once the user is updated in DEERS as an SSM, he/she must be updated through User Administration by adding the SSM role. The incoming SSM must terminate the outgoing SSM as a RAPIDS user at that site once the outgoing SSM officially leaves the site.

---

### 9.5 Site Administration

DEERS is the single point of entry for vital site information. DEERS shares this information with other systems that are critical to the installation, maintenance and support of RAPIDS. Additionally, with the automation of the automated card management system, CAC stock and supplies will be delivered only to the address stored in DEERS. These factors make the maintenance of site information such as addresses and telephone numbers ever more critical. SSMs should ensure that the two site addresses in RAPIDS are kept up to date (the mailing address and the location address, which specifies the address at which the SSM receives secure shipments, if different from the mailing address). Current Site Information is maintained by using the **Tools|Site Address** function. Please note, changes to Site Name, Site City and State must be requested through your Project Officer (see *Appendix C* for your SPO). Enhancements to this function include the use of two separate addresses, one for the receipt of regular mail and another for the signature receipt of CAC stock and supply deliveries.

Other site administration responsibilities include but are not limited to:

1. Administer the offline records generated by the VOs and SVOs at their site, including:
  - Viewing transaction errors.
  - Monitoring the offline records made by other VOs.
2. View or update RAPIDS Configuration Utilities found in *Section 9.3* of this training guide.
3. Notify the PO or DSO when a purge, invalid entry, or lock to a record is necessary.

4. Maintain the Site Roster (Keep the roster up to date by using the **Tools|User Administration** function).
5. Ensure a Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA) is established between the server and the remote site(s).

---

## **9.6 Documentation and training**

The SSM is responsible for the upkeep of current versions of related publications and articles, management of initial and continued training of site personnel and maintenance of current RAPIDS software and server-related settings. These tasks include:

1. Train new VOs and SVOs on the RAPIDS software using this Training Guide.
2. Train new VOs or SVOs on security policies using the RAPIDS Security SOP.
3. Train users on any existing MOU or MOA.
4. Fully train secondary or replacement SSM.
5. Ensure that all VOs and SVOs have read and understand the “Message of the Day.”
6. Download and install new RAPIDS software, as instructed.

---

## **9.7 Inventory Logistics Portal**

The Inventory Logistics Portal (ILP) automates the process for ordering Common Access Card (CAC) stock and tracking the usage levels for each site. The ILP is a Web-based CAC accountability system that the Site Security Manager (SSM) must use to manage the CAC stock for his/her site.

---

## **9.8 Using RAPIDS Configuration Utilities**

The RAPIDS Configuration Utilities application can be accessed by:

1. Selecting the **RAPIDS Configuration Utilities** icon on the Windows desktop.  
-or-
2. Selecting **Tools|Configuration** from the main menu from within RAPIDS.

Except for the *CAC* tab, which all users can access, RAPIDS SSMs and Administrators are the only users with authorization to change certain data while using the configuration screens within RAPIDS. The information is read-only for all other users. However, all users can use the test buttons once a device/database has been configured and all users can access the *CAC* tab to test or read information on a CAC. The following tabs are displayed: **System, Authentication, Readers, Camera, Databases, Printers, CAC, and Security**. Configuration information can only be changed by the RAPIDS SSM under the direction of the D/RAC / D/RSC-E / DSO-A, or

RAPIDS software developers. See *Section 6.11.5* of this training guide for detailed instructions on using the CAC options.

## 10 Deployable RAPIDS

---

### 10.1 Overview

Deployable RAPIDS is a laptop version of RAPIDS used in mobilizations or onboard U.S. Navy ships. When RAPIDS is loaded on a deployable workstation such as a laptop, the look-and-feel is similar to that of a desktop RAPIDS workstation that is designed to have constant communication with DEERS via a RAPIDS Server. Desktop RAPIDS workstations are designed to operate continuously in online mode (only disruptions to normal communications force a desktop workstation into offline mode). Deployable RAPIDS is designed to operate in either online or offline modes (called “Deployed mode”) for extended periods. **Note:** Deployable RAPIDS must be operating in online mode meaning a connection to the IP and CA exists to obtain the PKI certificates and encode them on the CAC.

This section is designed to familiarize users with the differences between deployable RAPIDS and desktop RAPIDS workstations. This section is organized as follows:

1. Before your unit deploys (READ NOW!)
2. Establishing communications on deployable RAPIDS
3. Deployable RAPIDS User Administration
4. Logging on to deployable RAPIDS
5. Creating ID cards using deployable RAPIDS
6. Deployable Data Storage and Transmission
7. Deployable RAPIDS theft protection and the Key Master

---

### 10.2 Before your unit deploys (Read now!)

To ensure that you use deployable RAPIDS correctly and quickly, we recommend that your unit understand the following steps, in advance, of any situation where you might be deployed.

1. Read this entire section and the RAPIDS Hardware Guide carefully with all the deployable hardware in front of you while you are reading, if practical. Note any questions or incompletely understood concepts. If you cannot find the answers to your questions in other portions of this manual, then contact the D/RAC / D/RSC-E / DSO-A for assistance (see *Appendix A* of this training guide).

2. Have a paper copy of the RAPIDS Training Guide and Hardware Guide ready during deployment. Remember Online help will not be available until you can successfully boot the laptop and start the RAPIDS application.
3. Read the manufacturer's user instructions for the hardware issued by your unit. The hardware information provided in the Hardware Guide is not designed to be a complete set of instructions. Make sure any manufacturer's instructions are in place with the deployable RAPIDS.
4. If possible, try using deployable RAPIDS in the mode you anticipate during deployment (preferably with communications) **before deployment**. This will allow you to use deployable RAPIDS successfully and will ensure the necessary coordination required for on-line communications with DEERS, the IP, and the CA during the deployment.

---

### 10.3 Establishing Communications for Deployable RAPIDS

Refer to the RAPIDS Hardware Guide for a hardware overview including setting up the RAPIDS system. Appendix M of this Training Guide provides the VO with tips on connecting the components. It is an excellent idea to try these procedures before your unit deploys, when there is certainty of communications, and when there is less pressure trying to establish communications for the first time in a deployed situation. Communications with DEERS, the IP, and the CA is required to produce CACs.

Three types of communications options are available to support RAPIDS workstation connectivity: (1) LAN connectivity via Ethernet, (2) dial-up connectivity via a centralized server/device, and (3) Defense Information System Network (DISN) 1-800 dial-up service. Each location that you operate your RAPIDS workstation from must be able to support one of these three communications methods and could vary by location, thus requiring re-configuration of the RAPIDS workstation prior to use. Please follow the steps outlined in *Sections 10.3.4* for Ethernet/LAN connectivity or *Section 10.3.5* for dial-up connectivity and take the appropriate actions to ensure connectivity to DEERS is available prior to arriving at the new issuance site. You will need to identify the Internet Protocol (IP) addresses, firewalls, Ethernet drops, analog phone lines, and/or logon IDs required to establish connectivity, as indicated for each method. Setting up the communications configuration for deployable RAPIDS requires you to log on to the laptop with an administrator account, according to the instructions in *Section 10.3.1*, below. **Note:** Any communication charges incurred (i.e., charges to install network drop or telephone line, telephone line usage charges, centralized dial-up accounts, etc.) are the responsibility of the RAPIDS operator's unit.

#### 10.3.1 Logging On to Deployable RAPIDS as Administrator

1. To perform communications configuration, you must log on with administrative privileges. If the system is powered on, close any programs that are running and log off the computer. Click on **Start**, then choose **Shut Down** from the menu, then choose the **Logoff (user ID)** option. Otherwise, power on the system.

5. Press the **Ctrl**, **Alt**, and **Delete** keys, simultaneously, to display the **Authorized Users Only** screen. At the end of the text, two codes appear in a single set of parenthesis. These are encrypted codes that contain the logon ID and password for the Administrator account on this computer.
6. Call the D/RAC / D/RSC-E / DSO-A (see Appendix A of this Training Guide for phone numbers) to get information to log on to your deployable RAPIDS as administrator. They will request the codes at the bottom of the **Authorized Users Only** screen and provide the one-time password for the Administrator account.
7. Click on **OK** to advance to the **Logon Information** screen.
8. Type the **logon ID** supplied to you by the D/RAC / D/RSC-E / DSO-A in the **User name** text box. **Note:** The User name is case sensitive.
9. Type the password supplied to you by the D/RAC / D/RSC-E / DSO-A in the corresponding text box, then click **OK**. You will be logged on with administrator permissions.

### 10.3.2 Adding a Machine Name

1. Logon with Administrative privileges.
2. Cable up all network cables if not already done.
3. Right click on the *My Computer* icon and select **Properties**.
4. Select the *Network Identification* tab (if needed) and verify the existing Computer Name and Workgroup.
5. Click the *Properties* button to rename the computer name or workgroup using the information provided by the DMDC Communications Team. **Note:** If both the Computer Name and the Workgroup need to be updated, this should be done in two separate steps as detailed in these instructions. Select **OK**.
6. Select **OK** at the message box, “The Computer Name has been successfully changed to [Computer Name]. This change will not take effect until the computer is restarted.”
7. Logon with Administrative privileges.
8. Right click on the *My Computer* icon and select **Properties**.
9. Select the *Network Identification* tab (if needed) and add the Workgroup name as follows:
10. Select the **Workgroup** radio button and type in the Workgroup as provided by the DMDC Communications Team.
11. Select **OK** on the *Identification Changes* dialog.

12. Select **OK** at the message box, “Welcome to the [Domain Name] domain.” Select **Close** within the Network dialog.
13. Select **Yes** at the message box, “You must shut down and restart your computer before the new setting will take effect. Do you want to restart your computer now?”.

### **10.3.3 Configuration for Ethernet/Local Area Network Communications**

RAPIDS workstations can connect to DEERS via a military installation's Ethernet/LAN, which is connected to DISN. It is not necessary to connect to a RAPIDS server, because DEERS will recognize the Deployable RAPIDS workstation just as it would recognize any RAPIDS server. To connect to DEERS in this type of setup, you will need an available LAN connection and an IP address. The installation's Communications Activity can provide these to you.

Expectations of the SSM in conjunction with the hosting facility where the RAPIDS system will be used:

1. Prior to using the RAPIDS equipment, the SSM will be responsible for ensuring the availability of a 10BaseT (uses twisted pair cabling) Ethernet LAN connection and an IP address for the location where they plan to operate the RAPIDS workstation. Dynamic Host Configuration Protocol (DHCP) is the preferred method of IP addressing. If DHCP is not available at the hosting facility, a static IP address within the domain of the hosting facility will be required. The RAPIDS user will be required to contact the D/RAC / DRSC-E / DSO-A to obtain the encrypted system administrator password (see *Section 10.3.1* of this training guide) to allow for the configuration described below.
2. If a firewall is installed at the site, the SSM in conjunction with the hosting facility will be responsible for ensuring that the following firewall ports are open: SSL 443 for pull/push of data and port 1521 for Oracle database synchronization.
3. The SSM should research the answers to the following questions before attempting to establish communications with DEERS using a network interface card (also called Network Adapter or NIC).
  - Does your site use DHCP or will you be given a static IP address with which to connect?
  - Will you be given a static IP address? If so, you need to get the Subnet Mask and Default Gateway, as well. All three are numeric codes that contain dots (for instance, static IP address 199.209.11.14, Subnet Mask 255.255.255.0, Default Gateway 199.209.11.1). Make sure you know where the dots are supposed to go – it could save you some needless frustration when it is time to enter these codes in their respective text boxes.
  - Is there a firewall in place? Consult with the local LAN/Systems Administration/Communications Point-of-Contact to determine this. If so, it is imperative that firewall port 443 (SSL) for pull/push of data and port 1521 for Oracle database synchronization are open.

The SSM will be responsible for configuring the RAPIDS device to connect to the LAN, prior to using the RAPIDS workstation. Instructions are contained in the Deployable RAPIDS Training

Guide Addendum provided on CD-ROM with the RAPIDS hardware.

After obtaining the above information, close all applications on Deployable RAPIDS.

1. Connect the network cable between the Ethernet LAN port on the RAPIDS laptop and the base LAN drop. This should be done prior to turning on laptop. See *RAPIDS Hardware Guide-Figure 4-2 Right Side* for details.
2. Log on using the Administrator account and password. Refer to *Section 10.3.1* of this training guide for additional instructions.
3. Right click the My Network Places icon from the desktop and select Properties. The Network and Dial-Up Connections window will be displayed.
4. Right click the Local Area Connection icon and select Properties. The Local Area Connection Properties dialog will be displayed.
5. Ensure that the Intel 8255x-based PCI Ethernet Adapter (10/100) is displayed in the *Connect using:* text box.
6. Highlight Internet Protocol (TCP/IP) from the list of components and select Properties. The Internet Protocol (TCP/IP) Properties dialog will be displayed.
7. For DHCP Ethernet connections,
  - There must be a properly configured DHCP server on the same network as the RAPIDS system for the DHCP configuration to function properly.
  - Select the option to obtain an IP address automatically if it is not already selected.
  - Skip to Step 9.
8. For static IP Ethernet connection,
  - Select the option **Use the following IP address** if it is not already selected.
  - Type in the IP address from the Site Information sheet. (Example: 159.227.50.128).
  - Type in the subnet mask from the Site Information sheet. (Example: 255.255.255.0).
  - Type in the default gateway IP address from the Site Information sheet. (Example: 159.227.50.1).
9. Click *OK* to close *Internet Protocol (TCP/IP) Properties* dialog.
10. Click *OK* to close *Local Area Connection Properties* dialog. Close the *Network and Dial-up Connections* window and log off. Click on **Start**, then choose **Shut Down from the menu list**, then choose the **Logoff (user ID)** option. **Note:** It is not necessary to reboot.
11. Log on to RAPIDS. Refer to *Section 5.3* of this training guide for log on procedures.



12. If RAPIDS does not auto-launch, double-click on the  icon to start RAPIDS. Check the status bar to verify you are connected. If the word *Deployed* appears, then double-click on it to establish the connection. You should now be online.

### 10.3.4 Updating Ethernet/LAN Configuration

Users of the Deployable RAPIDS systems running Windows 2000 have the option to change an IP address or switch between a DHCP and static IP address without logging on with administrative privileges.

1. Log on as a RAPIDS user. Administrative privileges are not necessary.
2. Select the *RAPIDS Configuration Utility* icon from the desktop.
3. Select the *Authentication* tab
4. Select the *Modify Local IP Configuration* button.
5. Ensure that the system is physically connected to the LAN before clicking **OK** at the *RAPIDS Configuration* dialog.
6. At the *TCP/IP Configuration* dialog, select the desired configuration (either *Obtain an IP from a DHCP server* or *Specify an IP address*).
7. Select **Update**.

### 10.3.5 Configuration for Dial-up Communications

For dial-up connectivity, it is necessary to dial-up to either a centralized dial-up server/device, Terminal Server Access Controller System (TSACS), or to the Defense Information System Agency (DISA)-provided 1-800 dial-up service.

#### 10.3.5.1 Dial up connectivity (Centralized Dial/TSACS):

RAPIDS workstations can connect to DEERS via a military installation's centralized dial device or TSACS. It is not necessary to connect to a RAPIDS server, because DEERS will recognize the Deployable RAPIDS workstation just as it would recognize any RAPIDS server. In order to connect to DEERS in this fashion, a user name and password must be assigned by the owner of the centralized dial-up device/TSACS along with a dial-up phone number. The installation's Communications Activity can provide these to you.

Expectations of the SSM in conjunction with the hosting facility where the RAPIDS system will be used:

1. Prior to receipt of the Deployable RAPIDS equipment, the SSM in conjunction with the hosting site will be responsible for ensuring the availability of an analog modem telephone line for each RAPIDS laptop.
2. The SSM in conjunction with the hosting facility will be responsible for obtaining a dial-up telephone number to access the base's centralized dial-up server/device or TSACS.
3. The SSM will be responsible for configuring the RAPIDS laptop to set up the dial-up phone number and update it whenever the centralized dial-up or TSACS server/device changes.
4. The SSM in conjunction with the hosting facility will be responsible for obtaining centralized dial-up or TSACS logon accounts and passwords.
5. If the base centralized dial-up or TSACS server/device resides inside the base firewall, the SSM in conjunction with the hosting facility will be responsible for ensuring that the following firewall ports are open: 443 (SSL) for pull/push of data and port 1521 for Oracle database synchronization.
6. The SSM will be responsible for configuring the RAPIDS device to dial-up to the appropriate centralized dial-up server/device, prior to using their deployable RAPIDS workstation, as outlined below.

### **10.3.5.2 Defense Information System Network 1-800 dial-up service**

Deployable RAPIDS workstations can connect to DEERS via the DISN 1-800 dial-up service provided by the DISA. This eliminates the need to connect to a RAPIDS server, because DEERS will recognize the RAPIDS laptop just as it would recognize any RAPIDS server. In order to connect to DEERS in this fashion, you will need a user name and password assigned to you by DISA that allows you to log into the DISN centralized dial-up device along with the toll-free telephone number. The installation's Communications Activity or DISA can provide these to you.

Expectations of the SSM in conjunction with the hosting facility where the RAPIDS system will be temporarily installed:

1. The SSM in conjunction with the hosting facility will be responsible for ensuring the availability of an analog modem telephone line for each RAPIDS laptop.
2. The SSM will be responsible for obtaining the DISN 1-800 dial-up number from DISA.
3. The SSM will be responsible for obtaining a DISN logon account and password from DISA and providing the appropriate funding associated with the logon account.
4. The SSM will be responsible for configuring the RAPIDS workstation to dial-up the appropriate DISN 1-800 dial number, prior to using their deployable RAPIDS workstation, as outlined below.

### 10.3.5.3 Creating a Dial-up Phonebook Entry

You can establish a dial-up connection with a modem any time while the deployable unit is in use, even during a RAPIDS session. If RAPIDS is running in deployed mode when you want to establish communications, go to step 1, below.

In order to succeed, you will need to know the telephone number of the modem at the centralized dial-up/TSACS or 1(800) DISA dial-up service location. You will need a user account for a centralized dial-up device that accepts incoming calls.

If you are attempting a dial-up connection on deployable RAPIDS and no Phonebook Entry exists for the system you are trying to dial into, you must create the Phonebook Entry using the following steps.

1. Right click on My Network Places icon and select Properties. The Network and Dial-Up Connections window will be displayed.
2. Double click on Make New Connection. The Network Connection Wizard dialog will be displayed.
3. Click on Next.
4. Select the option Dial-up to private network (default selection), then click Next to continue.
5. Type the telephone numbers you would have to dial on a telephone from your current location to connect to the centralized dial-up/TSACS Server. If you have to first dial "9" to get an outside line, include it during this step. Use a comma (,) to indicate a pause (e.g. to wait for a dial tone after dialing number(s) to get an outside line). If it is a long distance or international call, then include a "1" followed by the area/country code before the telephone number. Click *Next* to continue. Note: It is not necessary to select the Use dialing rules option. Select *Do not use my smart card*.
6. Leave the default selection For all users and click Next to continue.
7. Type a name (e.g. dial up to centralized device/server) for this entry in the provided text box, then click Finish.
8. A dialog will be displayed with the new dial-up entry, which is ready for use.

### 10.3.5.4 Establishing a Dial-up Connection

Verify Auto-Dial is disabled: (This step only needs to be done once)

1. From the Windows desktop, click *Start*, then select *Settings*, then *Control Panel*, then *Internet Options*. The *Internet Properties* window will be displayed.
2. Select the *Connections* tab.

3. Select the option *Never dial a connection* (if it is not already selected), then click the *OK* button to close the *Internet Properties* windows.

To dial-up using your modem, continue with the following steps:

1. Connect the telephone cable between the modem port on the RAPIDS laptop (see RAPIDS Hardware Guide for details) and the base phone jack.
2. From the Windows desktop, click Start, then select Programs, then Accessories, then Communications, then Network and Dial-up Connections. The Network and Dial-Up Connections window will be displayed.
3. Verify the name in the Phonebook Entry to dial-up is that of the server site you wish to connect to. If it is not displayed, click on the  button on the right side of the box and choose the correct entry from the list.
4. If the correct Phonebook Entry does not appear, you must add it to the list; this often occurs if your system has never connected to this particular centralized dial-up device/server. See the previous instructions in this section to create a Phonebook Entry.
5. When you make your Phonebook Entry choice, the values in the Phone Number Preview and Dialing From... boxes will be updated to contain the information that corresponds to the chosen entry.
6. Click Dial and the Connect to... window will be displayed. Type in the User Name and Password provided to you by the centralized/TSACS dial-up server site. Note: Do **not** select *Save Password*.
7. Click Dial again. The modem will attempt to connect.
8. If successful, the first time a dialog titled Connection Complete will be displayed. Select the check box Do not display this message again, then click OK. The window will close and an icon in the lower right corner of the Windows desktop will indicate a connection.



9. Double-click the  icon to start the RAPIDS application.

RAPIDS should come online at this point. However, if it does not, double-click on the word *Deployed* in the status bar. Click *Yes* to indicate that you want to establish the connection.

To delete a phone book entry, right-click the phonebook entry and select **Delete**.

---

## 10.4 Deployable RAPIDS User Administration

User administration on Deployable RAPIDS is significantly different from user administration on desktop systems. All users of deployable RAPIDS must have a user account that was created

on that deployable RAPIDS laptop to use the system. The subsections below describe the three aspects of user administration, which are particular to deployable RAPIDS.

### 10.4.1 Deployable RAPIDS and the SSM User Role

RAPIDS VOs require a CAC with LRA privileges to operate the system. Once a CAC is issued to a new VO, an SSM must request Local Registration Authority (LRA) privileges for that VO. Refer to *Section 9.2.1* of this training guide for instructions on adding new users with LRA privileges.

When any user account is created on deployable RAPIDS, the SSM role is automatically granted to that user as long as he or she is using that particular laptop. This means that, by default, all deployable RAPIDS users can add, modify and delete user accounts, and perform any of the other SSM functions while operating the system in deployed mode (i.e., without communications). The generic user account is also assigned the SSM user role (see *Section 9.2.2* of this training guide).

One important difference between desktop RAPIDS and Deployable RAPIDS relates to User Management. While desktop RAPIDS (with constant communications) are scheduled to refresh security information every evening, security information on Deployable RAPIDS requires a user to manually refresh security information as needed. If you have added a new VO, requested LRA privileges, updated or terminated a VO, or updated your site contact information, it is necessary to select *Tools|Refresh Security Information* the day after the request to refresh the updated information on the laptop.

#### 10.4.1.1 Creating and Registering User IDs on Deployable RAPIDS

For communications and security purposes, each deployable RAPIDS laptop is regarded as a RAPIDS site. In order for the records sent by a deployable RAPIDS user to be accepted by DEERS, the user's ID must be both:

1. created on that RAPIDS laptop, even if the user has an account that already exists at a desktop (non-deployable) RAPIDS workstation or on other deployable RAPIDS laptops; and
2. registered to be used at the RAPIDS site corresponding to the deployable RAPIDS workstation they will use.

There are two ways to set up an account on deployable RAPIDS as described below.

1. **Create and register DEERS user IDs in online mode ahead of time.** This is the **preferred method**, whenever it is possible, because you can create and register the user IDs when communications are available between deployable RAPIDS and DEERS. When you create a user ID on deployable RAPIDS, you can follow the normal procedure for creating a user ID at any desktop RAPIDS (see *Section 9.2.1* of this training guide). The user ID is in this case, registered automatically.

Therefore, when RAPIDS users who will use deployable RAPIDS are identified a few days before the deployment, connect the deployable laptop to DEERS, and create the user ID(s) on the deployable RAPIDS before the actual need arises.

2. **Create and register user IDs in offline mode.** This may be necessary if there is a need to add user IDs in deployed situations, when it is impossible to make a connection between deployable RAPIDS and DEERS.

Creation and registration of user IDs in offline modes require a form of verbal or message communications with the DEERS/RAPIDS Security Office or the D/RAC / D/RSC-E/DSO-A. If phone lines, e-mail or other communications are not available; it is not possible to use this method. Call the DEERS/RAPIDS Security Office at 1-800-3RAPIDS, ext. 5006/7 or 1-800-538-9522, ext. 5006/7; send e-mail (call and ask for the e-mail address), or send regular mail to 1600 N. Beauregard St., Attention: Security, Alexandria, VA 22311. Provide the reason for the call in addition to the following:

- The site ID of the deployable RAPIDS laptop for which the user needs to be registered (it appears in the first screen of the RAPIDS User Security Navigator) on your deployable workstation, choose **Tools|User Administration** from the RAPIDS menu bar to view it.
- Provide the name and Social Security Number of the person who will use the deployable RAPIDS.

This process requires 24 hours to complete. The site should call the D/RAC / DRSC-E / DSO-A, the following business day to obtain the Logon-ID that was assigned to the new user. These offices will provide two character strings, which should be typed into the *Encrypted Data and Description Key* text boxes when prompted to do so by the *RAPIDS User Security Navigator*.

Add the user account as you would normally add any user account, referring to the instructions in *Creating a RAPIDS User Account* in this Training Guide, if necessary. At the beginning of the navigator, an additional screen is displayed which prompts you to enter the Encrypted Data and Description Key. Fill in these fields with the character strings that were provided to you by the Security Office.

#### **10.4.2 Generic User ID on Deployable RAPIDS**

Each RAPIDS laptop is configured with a generic user account. This allows your unit to continue issuing ID cards and to perform other RAPIDS actions in the event that no one with a valid user ID is available. This generic ID can be obtained by calling the D/RAC / D/RSC-E/DSO-A.

When a user is logged on using the generic ID, he or she is not allowed to transmit data to DEERS. However, a generic user can work in offline mode, and the records created can be sent to DEERS later by a user whose ID has been registered.

Every unit should ensure that all personnel who use deployable RAPIDS knows the generic user ID and password to maintain the continuous ability to issue ID cards during deployment.

## 10.5 Logging on to Deployable RAPIDS

1. If the deployable RAPIDS laptop is turned off, ensure that any peripherals are properly connected to the laptop and turned on, before turning on the laptop.
2. Turn the laptop computer's power on and let the machine boot, if necessary. You are ready to proceed when the Begin Logon screen appears.

Refer to *Section 5.3* of this training guide for instructions on Logging on to RAPIDS.

**Note:** New users of the RAPIDS software are encouraged to review the *RAPIDS Training Guide* in its entirety to become familiar with basic RAPIDS tasks such as opening a family, updating sponsor and family records. This is covered in detail within *Section 7* of this training guide. For your convenience, instructions for creating the DD Form 1172 and the ID Card are shown in the following sections.

---

## 10.6 Creating ID Cards Using Deployable RAPIDS

Deployable RAPIDS can be used to create all types of ID cards when it is connected to DEERS. When in deployed mode, however, you can only use it to create Non-chip cards for **Active Duty**, **Select Guard/Reserve**, and **Civilian Geneva Conventions ID cards** (The process of ID card creation on deployable RAPIDS is similar to that for creating an ID card on a RAPIDS desktop workstation. Refer to *Section 7.46.2* of this training guide for instructions.

**Note:** If your deployable RAPIDS is in the deployed mode, ID cards are restricted to Non- ICC CACs for Active Duty, Guard/Reserve, DoD Contractor, and DoD Civilians.

---

## 10.7 Deployable Data Storage and Transmission

When you are using a desktop (non-deployable) RAPIDS workstation, any records in offline storage are automatically sent to DEERS every thirty minutes, as long as your workstation maintains its connection to DEERS. There is no automatic transmission process for deployable RAPIDS. Users of deployable RAPIDS must manually instruct RAPIDS to send the records in the off-line repository to DEERS. Additionally, deployable users must make the following decision, based upon the anticipated availability or unavailability of communications:

1. Should the records all be kept in offline storage because communications will be available within a reasonable period?
2. Should the records be saved in an archive file that can be sent to a non-deployable RAPIDS site, who will in turn transmit the records to DEERS?

Three menu bar commands enable both deployable and desktop RAPIDS users to perform these functions.

1. **File|Repository|Upload** menu command allows deployable RAPIDS users to transmit any family records in the offline storage repository to DEERS. The records are then deleted from offline storage. You must log on with communications established to use this command.
2. **File|Repository|Export** menu command combines all family records that are currently contained in the offline repository into an archive file that you can choose to save on the deployable RAPIDS hard drive or to floppy disk if a portable floppy drive is installed in/or connected to the laptop computer. The command then gives you the option of clearing the offline repository, so that duplicate records do not exist, or to let the records remain in offline storage (if you want to use the archive files just as a backup) and transmit them to DEERS directly.
3. **File|Repository|Import** menu command reads the exported (archive file) family records (as described above), back into the offline repository so they can be transmitted to DEERS. In order for this command to succeed, sufficient space must be available in offline storage (on the laptop's hard drive) to hold the records contained in the archive.

### 10.7.1 Uploading from Offline Repository to DEERS

In order to transmit the records that are currently in deployable RAPIDS offline storage repository to DEERS, you must take the following steps:

1. Establish communications with DEERS (refer to *Section 10.3* of this training guide).
2. Choose **File|Repository|Upload** from the menu bar. The Upload Off-line Records window will open.
3. Type your DEERS/RAPIDS user ID and password into the corresponding text boxes, then click on the Upload button. A DOS window will open, showing the execution of the upload program. Remember your user ID and password must be registered on the RAPIDS server to which you are connected in order to upload offline records from the deployable RAPIDS storage repository.
4. The time required for the upload to complete can vary widely, primarily as a function of the number of records being uploaded and the quality of the communications connection, and therefore speed of the connection. Upload times of less than a minute, or of over an hour, are both possible. You can continue to use your deployable workstation in the meantime, by clicking on the DOS window's  button to minimize it. CAUTION: Do not click on the  button; it will stop the communications program from completing the data transmission to DEERS.

### 10.7.2 Exporting Records to an Archive File

Follow these steps to save the records in your deployable RAPIDS offline repository to a RAPIDS data archive file. This archive file can later be reloaded into the offline storage repository (through your deployable RAPIDS or desktop RAPIDS workstation) and the records

then sent to DEERS. You do not need connectivity to DEERS to create an archive file.

1. Choose File|Repository|Export from the menu bar. A popup window asks you to confirm that you want to export your offline records. Click on Yes. A standard Windows Save As... dialog box will appear.
2. Save the archive to either your hard drive C: (if you anticipate sending the records in this archive to DEERS from deployable RAPIDS when communications become available) or to a floppy disk by choosing A: in the Save in box. Remember the floppy drive must be installed in/or connected to the laptop (same port as you would use for the printer) before you boot deployable RAPIDS, so Windows can detect it. Saving the archive on a floppy disk gives you the option of sending it to a desktop RAPIDS site for transmission to DEERS.
3. Give the archive file a name by typing the name into the File name box. The default extension is .roa.
4. Click on Save. If a file is too large to fit on one floppy disk, the user will be prompted to insert another floppy.

### 10.7.3 Importing an Archive File into Offline Storage

Once RAPIDS storage repository data has been exported to an archive file it can then be imported back into offline storage. An example of this is to export data from deployable RAPIDS workstation and import it to a desktop RAPIDS workstation, so that the data can be forwarded to DEERS. You do not need connectivity to DEERS in order to read the contents of an archive file into offline storage.

1. Choose File|Repository|Import from the RAPIDS menu bar. The standard Windows 2000 (deployable RAPIDS) or Windows NT (desktop RAPIDS) Open window is displayed.
2. Choose the device (e.g. A: for floppy disk, C: for hard drive:) and directory where the archive is located. RAPIDS offline archives have a .roa filename extension.
3. Click on Open. A popup window will notify you that the import was successful; click on OK to close the notification popup.

**Note:** When an archive is read back into offline storage, the duplicate records already contained in offline storage, are not "dropped." This can cause duplication of records in offline storage.

---

## 10.8 RAPIDS Theft Protection and the Key Master

RAPIDS deployable systems run a much higher risk of theft than desktop workstations. It is expected that desktop workstations be used in secured areas, whereas deployable units are frequently used in public spaces. Because of this increased risk, the deployable workstations are required to have an extra layer of protection against unauthorized use.

All dedicated RAPIDS systems have a watchdog program that monitors the use of the system.

This program must be resident in memory for RAPIDS to run. On deployable workstations, the watchdog program is extended in an attempt to minimize the amount of time a system can be used without authorization. Much of the increased security relies on the fact that the system will lock itself after a certain number of days until a *Key Master* provides the appropriate key to unlock it.

A locked system will not allow the RAPIDS application to run. Users will still be able to log on to Windows 2000, but they will be prompted that the use of RAPIDS is suspended. If a user tries to run RAPIDS while the system is locked, a message box appears with the message, "The security system of this dedicated RAPIDS machine has been compromised. Please contact the DEERS/RAPIDS Assistance Center for more details. RAPIDS will now exit." The *Key Master* and a Windows administrator are the only individuals who can unlock a system. The *Key Master* should therefore be a ranking official who is responsible for ensuring that the deployable system is being used for authorized card issuance.

Locking the system after a specified number of days should minimize the amount of time that a stolen system could be used to create fraudulent ID cards. Of course, to create ID cards on a stolen system, the thief would also need to have stolen user credentials, CAC, and cardstock. If the thief has stolen the *Key Master* password, then the fact that the system resets after the number of unlocks has been exceeded, should minimize the amount of time that a stolen system could be used to create fraudulent ID cards. The system must be reset after the specified number of unlocks (default is ten) has been exceeded. Only a Windows administrator can reset the system.

### 10.8.1 Key Master password

If the *Key Master* password does not exist or a program other than those approved by RAPIDS created it, the user will receive the message box; "The security of this dedicated RAPIDS system has been compromised. Use of RAPIDS on this system will be suspended".. After acknowledging the message box, the user is unable to use RAPIDS. New deployable systems are created with a default password.

If the system has been configured to lock up after a certain number of days and the number of times that the system has been configured to allow unlocks has been reached, the user is prompted with the message box; "Use of RAPIDS has been suspended because the lockout period (X days) has been exceeded and the maximum number of Key Master unlocks (X) has been reached". The system must be reset by selecting a new Key Master password."

The user should ask the *Key Master* to enter the password. The *Key Master* is given three attempts to enter the correct password. If an incorrect password is entered three times, the *Key Master* receives the message box; "The password entered does not match the Key Master password. Use of RAPIDS on this system will be suspended". After acknowledging the message box, the user is unable to run the RAPIDS application. If this happens, the site must contact the D/RAC / D/RSC-E / DSO-A for assistance (see Appendix A of this Training Guide for contact information).

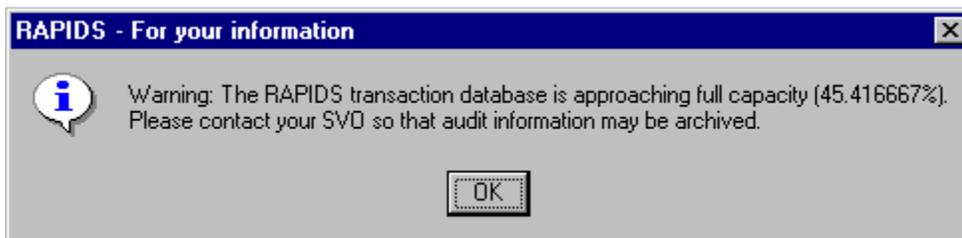
### 10.8.2 Setting the Key Master password

The site should designate one individual as the Key Master. The password for the Key Master can be set during your initial training when you receive deployable RAPIDS or by contacting the D/RAC / D/RSC-E / DSO-A for your region. The D/RAC / D/RSC-E / DSO-A will assist the user in setting the Key Master password by allowing the user temporary administrator access. The lock-up should be adjusted to 45 days, and a six to eight character unique Key Master password should be entered to prompt the RAPIDS application to lock-up every 45 days. The Key Master and a Windows administrator are the only individuals who can unlock the system. If a site finds that the system is locked and the Key Master is no longer available or has forgotten the password, the site must contact the D/RAC / D/RSC-E / DSO-A for assistance (see Appendix A of this Training Guide for contact information).

---

### 10.9 Deployable RAPIDS Limit to Offline and Audit trail Database Size

If you see the warning message shown below, when you attempt to log on to deployable RAPIDS, it means your system's offline storage repository is full beyond the warning threshold that you (or another user of this deployable RAPIDS) have specified.



RAPIDS will allow you to continue saving records after this message appears, until the storage repository is full. You can decide between one of two courses of action, so that the warning message no longer appears.

1. **Connect and upload the records to DEERS:** When the records are transmitted to DEERS, the storage repository on your laptop computer is emptied automatically. After uploading records, you can delete audit trail data, as necessary, to free up space on the hard drive.
2. **Set the warning threshold higher:** In the Databases tab of the **Tools|Configuration** menu, click on the **Advanced** button near the top (in the Transaction Database section). Adjust the percentage that appears in the bottom (in the Advanced Settings section).

## Appendix A - Quick Reference Guide

Please print and complete this section.

Server IP Address \_\_\_\_\_ Server Site/Phone \_\_\_\_\_

Workstation IP Addresses \_\_\_\_\_

### Help Desks

#### CONUS, Alaska, Hawaii, Virgin Islands, Cuba, and Puerto Rico

DEERS/RAPIDS Assistance Center

(800) 3-RAPIDS or (800) 372-7437

DSN: 761-6953/4/5/6/7

Hours: M-F 0700 EST - 2000 EST | Sat-Sun 0800 EST - 1700 EST (except U.S. Government holidays)

For assistance on hardware, software, security, communication, or application questions.

Direct Number to DEERS Security: (703) 578-5006/5007

#### European Theater

DEERS/RAPIDS Support Center - Europe:

Commercial Phone: 011-49-6371-867365

FAX: 011-49-6371-867672

DSN: 486-7365

DSN FAX: 486-7672

John Corrin

+49 (0)6371 86 7766

DEERS/RAPIDS Landstuhl, Germany

European Support Office

DSN (314) 486-7766

jcorrin@eso.lrmc.amedd.army.mil

FAX (314) 486-7672

#### Western Pacific Theater

DMDC Support Office (DSO) – Asia/Pacific (Seoul, Korea)

Comm: 011-822-7914-6195

DSN: 724-6195

Fax1: 011-822-795-1092 | Fax2: 011-822-7914-6204

DSN Fax: 724-6204

Hours: M-F 0800 - 1700 Local Time (except U.S. Government holidays)

Bob Miles

(822)7914-6195

DEERS/RAPIDS Asia/Pacific

DSN 724-6195

Asia/Pacific Support Office

FAX (822)795-1902

milesr@usfk.korea.army.mil

DSN Fax 724-6204

#### Verifying Official Information System (VOIS) Web Site

DMDC invites all RAPIDS users to access the new Verifying Officials Information System (VOIS) web site. The VOIS provides RAPIDS Verifying Officials (VO's) with quick and easy access to real-time systems information, up to date program information and many other resources such as archived Messages of the Day (MOTD), Points of Contact, links to other web sites and more. To access the VOIS simply select Tools|Web|VO Information System from the RAPIDS menu.

From a non-RAPIDS computer, type, <https://www.dmdc.osd.mil/vois/owa/vois>.

Our goal for this Website is to provide instant systems status and current RAPIDS/CAC information to all RAPIDS VOs.

### General Information

The **DEERS/RAPIDS Operations Division (D/R Ops Div)** is responsible for managing the DEERS/RAPIDS program. If you have questions about site implementation, hardware/software, training, or equipment, please contact:

Defense Manpower Data Center (DMDC)  
Attn: DEERS/RAPIDS Operations Division  
1600 Wilson Blvd. Suite 400  
Arlington, Virginia 22209-2593  
Comm: (703) 696-2000/2001  
DSN: 426-2000/1  
Fax: (703) 696-4107  
DSN Fax: 426-4107

The **DMDC Support Office (DSO)** conducts DEERS record research. For research on a DEERS record or mailing the DD Form 1172, please contact:

DMDC Support Office (DSO)  
Attn: Research and Analysis  
400 Gigling Road, 5th Floor  
Seaside, California 93955-6771  
Comm: (831) 646-1010 or (831) 583-2500  
DSN: 878-3261/2659/3335

### DSO Research and Analysis (R&A)

Contact DSO R&A for assistance with record problems or data discrepancies requiring an Invalid Entry Transaction.

Comm: (800) 361-2508  
DSN: 878-3522/3523

Beneficiaries with questions or problems concerning DEERS enrollment or TRICARE claim denials should please contact:

DMDC/DEERS Beneficiary Telephone Center

All Other States: (800) 538-9552

Hours: M-F 0600 PST - 1530 PST (except U.S. Government holidays)

VOs that have a DEERS log on ID and password and need to verify the eligibility of sponsors and family members should please contact:

DEERS Eligibility Telephone Center

Comm: (800) 368-4416 or (800) 336-0289

DSN: 837-6299

Hours: M-F 0700 PST - 1500 PST (except U.S. Government holidays)

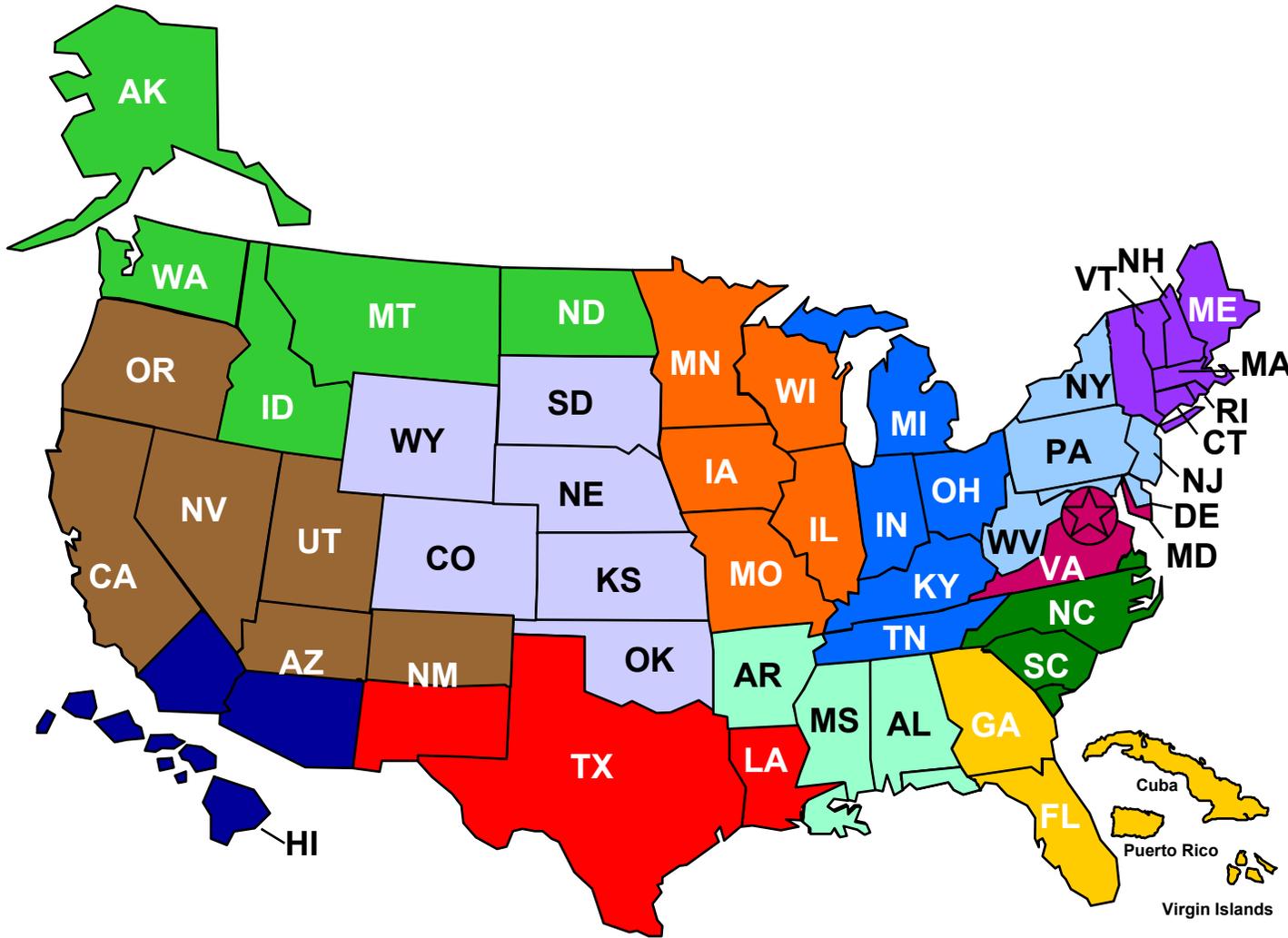
In an effort to improve the quality of service to our overseas customers, the DMDC Support Office in Seaside, CA has acquired toll free telephone numbers for DEERS eligible customers living in Germany, Italy, Philippines, United Kingdom, Korea and Japan. Customers can now call the DEERS Beneficiary Center in Seaside, CA to confirm their correct address is on file, all family members are properly enrolled on DEERS or they may inquire about any eligibility questions they may have. The following phone numbers can only be dialed from the country that they are assigned to.

Germany	-	0800-1013161
Italy	-	800-783784
Japan	-	00531-1-20731
Korea	-	00798-14-800-5570
Philippines	-	1-800-1-114-1235
United Kingdom	-	08-005871594

The Beneficiary Center hours of operation are from 6:00 AM to 3:30 PM PST, Monday - Friday, except on Federal Holidays. These phone numbers are for customer use only and VOs should not attempt to contact Research and Analysis using these numbers. The customer service representative will not be able to transfer your call.

Customers may also update their home address on DEERS via the Internet at <http://tricare.osd.mil/deers>.

# DEERS/RAPIDS Field Service Representatives



**Northwest (NW)**  
Joe Miller  
DEERS/RAPIDS Field Rep  
62nd MSS/DPMP  
100 Main Street, Suite 1033A  
McChord AFB, WA 98438  
(253) 982-2553  
DSN 382-2553  
FAX (253) 982-3039  
E-mail:  
millerjb@osd.pentagon.mil

**West (WC)**  
Erin Haas  
DEERS/RAPIDS Field Rep  
DSO  
400 Gigling Road  
Seaside, CA 93955-6771  
(831) 583-2500 ext.  
DSN 878-3261  
FAX (831) 373-1228  
E-mail:  
Haaseew@osd.pentagon.mil

**Pacific (PA)**  
Brian Roberts  
DEERS/RAPIDS Field Rep  
NMCSD-Region Nine TRICARE  
34960 Bob Wilson Drive  
Bldg. 6, Suite 400  
San Diego, CA 92134-6400  
(619) 532-7185  
DSN 522-7185  
FAX (619) 532-7172  
E-mail:  
roberthb@osd.pentagon.mil

**Rocky Mountain (RM)**  
Ricardo Maytorena  
DEERS/RAPIDS Field Rep  
TRICARE Central Region  
Building 1011, Specker Ave.  
Fort Carson, CO 80913  
(719) 524-2619  
DSN 883-2619  
FAX (719) 524-2653  
E-mail:  
maytorra@osd.pentagon.mil

**Southwest (SW)**  
Ed Yoder  
DEERS/RAPIDS Field Rep  
PASBA  
1750 Greeley Road  
Building 4011 Room 101  
Ft. Sam Houston, TX 78234  
(210) 221-2636  
DSN 471-2636  
FAX (210) 221-9016  
E-mail:  
yodered@osd.pentagon.mil

**South (SO)**  
Cyndi Aviles  
DEERS/RAPIDS Field Rep  
314 MSS/DPMP  
1255 Vandenburg, Suite 116  
Little Rock, AR 72099  
(501) 987-8960  
DSN 731-8960  
FAX (501) 987-7932  
E-mail:  
avilescj@osd.pentagon.mil

**Midwest (MW)**  
Pauletta Newett  
DEERS/RAPIDS Field Rep  
U.S. Army Reserve Center  
4301 Goodfellow Boulevard  
St. Louis, MO 63120-1794  
(314) 898-4000 x4230  
866-366-3346 x4230  
FAX (314) 263-2761  
E-mail:  
newettpr@osd.pentagon.mil

**Great Lakes (GL)**  
Peter Puro, Jr.  
DEERS/RAPIDS Field Rep  
127th MSS/DPM  
Building 304  
Selfridge ANG Base, MI 48045  
(586) 307-5625  
(586) 307-5625  
DSN 273-5625  
FAX (586) 307-6240  
E-mail:  
purolpj@osd.pentagon.mil

**Mid-Atlantic (MA)**  
LuAnn Seidenstricker  
DEERS/RAPIDS Field Rep  
193rd Civil Engineering Squadron  
78 Mustang Alley, Room 137  
Middletown, PA 17057-5078  
(717) 948-2481  
(717) 948-2481  
DSN 423-2481  
FAX (717) 948-2531  
E-mail:  
seidenln@osd.pentagon.mil

**Field Rep Consultant**  
Fred Stark  
DEERS/RAPIDS Field Rep  
6 MSS/DPM  
8011 Tampa Point Blvd.  
MacDill AFB, FL 33621-5321  
(813) 828-9714  
(813) 828-9714  
DSN 968-9714  
FAX (813) 828-2277  
E-mail:  
starkfh@osd.pentagon.mil

**Southeast (SE)**  
Denise Hutchins Trevino  
DEERS/RAPIDS Field Rep  
43rd MSS/DPMP  
384 Maynard Street  
Pope AFB, NC 28308-2374  
(910) 394-4744  
(910) 394-4744  
DSN 424-4744  
FAX (910) 394-4747  
E-mail:  
hutchida@osd.pentagon.mil

**Manager, Field Operations**  
Lou Leach  
(703) 578-5245  
E-mail:  
leachml@osd.pentagon.mil

**Field Rep Consultant**  
\*Sangeeta Ryan  
(703) 578-5309  
E-mail:  
ryansd@osd.pentagon.mil

**Gulf Coast (GC)**  
TBD

**Capital**  
\*Jay Anderson  
(703) 578-5310  
E-mail:  
andersjs@osd.pentagon.mil

**Northeast**  
\*Suellen Black  
(703) 578-5211  
E-mail:  
blacksn@osd.pentagon.mil

\*DEERS/RAPIDS  
1600 N Beauregard St., Ste. 100  
Alexandria, VA 22311  
DSN 761-6953/7  
FAX (703) 578-5325

**Europe**  
John Corrin, Manager  
EDS DEERS/RAPIDS Supt Ctr.  
US Hospital/ AM Kirchberg  
1st Street, Geb 3701, 2-OG  
66849 Landstuhl Germany  
011-49-6371-86-7365  
DSN 486-7365  
FAX 011-49-6371-86-7672  
E-mail:  
jcorrin@eso.lrmc.amedd.army.mil

**Western Pacific**  
Bob Miles, Manager  
HHC, 8th PERSCOM  
Attn: DRSC-W  
APO, AP 96205-0089  
011-822-7914-6195/6/7/8  
DSN 724-6195  
FAX 011-822-795-1092  
E-mail:  
milesr@usfk.korea.army.mil

**FSR**  
Andrea Deshayre  
DEERS/RAPIDS Field Rep  
62nd MSS/DPMP  
100 Main Street, Suite 1033A  
McChord AFB, WA 98438  
(253) 982-8458  
DSN 382-8458  
FAX (253) 982-3039  
E-mail:  
deshayaj@osd.pentagon.mil

## **Appendix C – Joint Uniformed Services Personnel Advisory Committee**

### **Army (USA)**

Ms. Cynthia Sublett  
HQDA (TAPC-PDO-IP)  
200 Stovall Street  
Hoffman Building 2, Room 3S49  
Alexandria, VA 22332-0474  
Comm: (703) 325-0202//9590  
DSN: 221-0202/9590  
FAX: (703) 325-4532  
E-mail: [sublette@hoffman.army.mil](mailto:sublette@hoffman.army.mil)

Ms. Jacquelin Hines  
Comm: (703) 325-4525/9590  
DSN: 221-4525/9590  
E-mail: [hinesj@hoffman.army.mil](mailto:hinesj@hoffman.army.mil)

### **Navy (USN)**

LT Robert Cross, USN  
Navy Personnel Command  
PERS 322, Building 769  
5270 Integrity Drive  
Millington, TN 38055-3320  
Comm: (901) 874-3056  
DSN: 882-3056  
FAX: (901) 874-2640  
DSN FAX: 882-2640  
E-mail: [p33D@persnet.navy.mil](mailto:p33D@persnet.navy.mil)

### **Doris Perry**

Comm: (901) 874-3467  
DSN: 882-3467  
E-mail: [p332b@persnet.navy.mil](mailto:p332b@persnet.navy.mil)

### **Marine Corps (USMC)**

Ms. Mary Stroz  
3280 Russell Road  
Code MRP1  
Quantico, VA 22134  
Comm: (703) 784-9529/9530/9531/9532  
DSN: 278-9529/9530/9531/9532  
FAX: (703) 784-9827  
E-mail: [strozm@manpower.usmc.mil](mailto:strozm@manpower.usmc.mil)

Ms. Norma Reiter  
E-mail: [ReiterNL@manpower.usmc.mil](mailto:ReiterNL@manpower.usmc.mil)

### **Air Force (USAF)**

Mr. George Hoback  
HQ AFPC/DPSFR  
550 C Street W., Suite 37  
Randolph AFB, TX 78150-4739  
Comm: (210) 565-2089/2467  
DSN: 665-2089/2467  
FAX: (210) 565-2543  
E-mail: [george.hoback@randolph.af.mil](mailto:george.hoback@randolph.af.mil)

**AFPC Call Center (Customer Service Personnel Calls)**

DSN: 665-7849 | FAX: (210) 565-2543

**Coast Guard (USCG)**

CWO2 Connie K. Rapp  
DEERS/RAPIDS Project Officer  
Commandant (G-WPM-2)  
2100 Second Street, SW  
Washington, DC 20593-0001  
Comm: (202) 267-2257  
FAX: (202) 267-4823  
E-mail: [crapp@comdt.uscg.mil](mailto:crapp@comdt.uscg.mil)

**Public Health Service (PHS)**

Mr. Norman Chichester  
Officer Development Branch, DCP  
Parklawn Building, Room 4-35  
5600 Fishers Lane  
Rockville, MD 20857  
Comm: (301) 594-3393  
FAX: (301) 594-2711 / (301) 443-6730  
E-mail: [nchichester@psc.gov](mailto:nchichester@psc.gov)

**National Oceanic and Atmospheric Administration (NOAA)**

Mr. Steve Eisenberg  
1315 East West Highway  
SSMC #3, Room 12100  
Silver Spring, MD 20910  
Comm: (301) 713-3453 (ext. 102)  
FAX: (301) 713-4140  
E-mail: [steve.eisenberg@noaa.gov](mailto:steve.eisenberg@noaa.gov)

**OSD Reserve Affairs (OSD/RA)**

COL James Scott  
Program Manager DEERS/RAPIDS  
OASD/RA (M&P)  
1500 Defense Pentagon  
Washington, DC 20301-1500  
Comm: (703) 693-7490  
FAX: (703) 695-3659  
E-mail: [jscott@osd.pentagon.mil](mailto:jscott@osd.pentagon.mil)

**Army National Guard (USARNG)**

Ms. Judith Mitchell  
ARNG Readiness Center  
ATTN: NGB-ARP-PC  
111 South George Mason Drive  
Arlington, VA 22204-1382  
Comm: (703) 607-9194  
DSN: 327-9194  
FAX: (703) 607-7184  
E-mail: [judith.mitchell@ngb.army.mil](mailto:judith.mitchell@ngb.army.mil)

**Army Reserve (USAR)**

Mr. Terry Rowles  
US Army Reserve Personnel Command  
1 Reserve Way  
St. Louis, MO 63132-5200

Comm: (314) 592-1041  
DSN: 892-1046  
E-mail: [terry.rowles@arpstl.army.mil](mailto:terry.rowles@arpstl.army.mil)

**Air National Guard (USANG)**

MSgt Gary Jackson  
ANG/DPFOC  
1411 Jefferson Davis Highway  
Arlington, VA 22202-3231  
Comm: (703) 607-1239 | DSN: 327-1239  
DSN FAX: 327-1066  
E-mail: [Gary.Jackson@ngb.ang.af.mil](mailto:Gary.Jackson@ngb.ang.af.mil)

**Coast Guard Reserve (USCGR)**

CW02 William Tubbs  
USCGR PO  
HQ, U.S. Coast Guard (HTR)  
2100 Second Street, SW, Room #5100  
Washington, DC 20593-0001  
Comm: (202) 267-1603  
FAX: (202) 267-4243  
E-mail: [wtubbs@comdt.uscg.mil](mailto:wtubbs@comdt.uscg.mil)

**Navy Reserve (USNR)**

PNC(SW) Darlene Anderson  
Commander, Naval Reserve Force  
ATTN: N12  
4400 Dauphine Street  
New Orleans, LA 70146-5000  
Comm: (504) 678-6053 | DSN 678-6053

FAX: (504) 678-6272  
DSN FAX: 678-6272  
E-mail: [ANDERSDA@cnrf.navy.mil](mailto:ANDERSDA@cnrf.navy.mil)

YN1 Jean Kaszantis  
Comm: (504) 678-6139  
DSN: 678-6139

**Air Force Reserve (USAFR)**

Col Dave Percich  
HQ, USAF/REPP  
1150 Air Force Pentagon  
Washington, DC 20330-1150  
Comm: (703) 588-6002  
DSN: 425-6002  
FAX: (703) 588-8444/8  
E-mail: [david.percich@re.hq.af.mil](mailto:david.percich@re.hq.af.mil)

**Air Reserve Personnel Center (ARPC)**

(20 yr. Letters/Survivor Benefits)  
(800) 525-0102 x227  
DSN: 926-6438 (Rhonda) | 926-6576 (Darrel Grunius)

**Marine Corps Reserve (USMCR)**

LtCol Ivan Glasco  
Commander MARFORRES, Code 7AA  
4400 Dauphine Street  
New Orleans, LA 70146-5400  
(504) 678-6584  
FAX: (504) 678-6584  
DSN: 678-6584  
DSN FAX: 678-1082  
E-mail: [glascoi@mfr.usmc.mil](mailto:glascoi@mfr.usmc.mil)

## **Appendix D – Joint Uniformed Services Medical Advisory Committee**

### **Army (USA)**

Mr. Alton Clark  
U.S. Army Medical Command  
2050 Worth Road - ATTN: MCHO-CL-P  
Fort Sam Houston, TX 78234-6000  
Comm: (210) 221-6113/6631  
DSN: 471-6113/6631  
FAX: (210) 221-6630  
E-mail: [alton.clark@amedd.army.mil](mailto:alton.clark@amedd.army.mil)

### **Navy (USN)**

Mr. Skip Katon  
Patient Administration/TRICARE Operations  
Bureau of Medicine and Surgery, Department of the Navy (M3M12)  
2300 E. Street, NW  
Washington, DC 20372-5300  
Comm: (202) 762-3144  
DSN: 762-3144  
FAX: (202) 762-3743  
E-mail: [fakaton@us.med.navy.mil](mailto:fakaton@us.med.navy.mil)

### **Air Force (USAF)**

Mr. Michael A. Harrison (PAHM)  
Deputy Chief, Managed Care Division, USAF  
HQ USAF-SGMA  
110 Luke Avenue, Room 400  
Bolling AFB, DC 20332-7050  
Comm: (202) 767-4726  
DSN 297-4726  
FAX: (202) 767-7366 | DSN 297-7366  
E-mail: [michael.harrison@pentagon.af.mil](mailto:michael.harrison@pentagon.af.mil)

### **Coast Guard (USCG)**

Mr. Terry Strickland  
Commandant Headquarters Coast Guard (G-WKH-3)  
2100 Second Street, SW  
Washington, DC 20593-0001  
Comm: (202) 267-0835  
FAX: (202) 267-4685  
E-mail: [wstrickland@comdt.uscg.mil](mailto:wstrickland@comdt.uscg.mil)

### **National Oceanic And Atmospheric Administration (NOAA)**

CAPT Michael Vitch  
NOAA/OMAOx1MV  
1315 East-West Highway, Room 12734  
Silver Spring, MD 20910  
Comm: (301) 713-3440 (ext. 186) FAX: (301) 713-2887

**Uniformed Services Family Health Plan (USFHP)**

Ms. Daphne Floyd  
OASD (HA) TMA/MHSO/SP&D  
Skyline 5, Suite 810A  
5111 Leesburg Pike  
Falls Church, VA 22041-3206  
Comm: (703) 681-0039  
DSN: 761-0039  
FAX: (703) 681-1219  
E-mail: daphne.floyd@tma.osd.mil

**Public Health Service (PHS)**

CAPT Anna Marie Balingit-Wines  
Chief, Beneficiary Medical Program,  
Medical Affairs Branch  
5600 Fishers Lane, Room 4C06  
Rockville, MD 20857  
Comm: (301) 594-6330  
FAX: (301) 594-2973  
E-mail: abalingit@psc.gov

**Medical System (Technical)**

Tri-Service  
Tri-Service Medical Systems Support Center (TMSSC)  
Help Desk  
Toll Free: 1-800-600-9332  
Comm: (210) 536-4150  
DSN: 240-4150

## Appendix E - RAPIDS Acronyms

AD	Active Duty
AHSMC	Auburn Hills Service Management Center
API	Application Programming Interface
CA	Certification Authority
CAC	Common Access Card
CD-ROM	Compact Disk – Read Only Memory
CHAMPUS	Civilian Health and Medical Program of the Uniformed Services
CHCS	Composite Health Care System
CICS	Customer Information Control System
CIN	Civilian Identification Number
CONUS	United States
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DD Form	Department of Defense Form
DEERS	Defense Enrollment Eligibility Reporting System
DHCP	Dynamic Host Configuration Protocol
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DMDC	Defense Manpower Data Center
DN	Distinguished Name
DNA	Deoxyribonucleic Acid
DOB	Date of Birth
DoD	Department of Defense
DoDI	Department of Defense Instruction
DOLI	DEERS Online Inquiry
D/RAC	DEERS/RAPIDS Assistance Center
D/R Ops Div	DEERS/RAPIDS Operations Division
D/RSC	DEERS/RAPIDS Support Center
D/RSC-E	DEERS/RAPIDS Support Center – Europe
DSO	DMDC Support Office
DSO-A	DMDC Support Office – Asia/Pacific
DTF	Dental Treatment Facility
EDI	Electronic Data Interchange
EDIPI	Electronic Data Interchange Person Identifier
FIN	Foreign Identification Number
FPKI	(US) Federal Public Key Infrastructure
FSR	Field Service Representative
FTP	File Transfer Protocol
GCA	Generic Container Applet
HIV	Human Immune-deficiency Virus
HP	Hewlett Packard
HV	High-Volume
ICC	integrated circuit chip

ID	Identification
IO	Issuing Official
IP	Internet Protocol/Issuance Portal
JDM	Joint Data Model
JSM	Joint Service Marriage
JUSPAC	Joint Uniformed Services Personnel Advisory Committee
JUSMAC	Joint Uniformed Services Medical Advisory Committee
LAN	local area network
LRA	Local Registration Authority
MIA	Missing in Action
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MSC	Military Sealift Command
MTF	Medical Treatment Facility
MWR	Morale, Welfare, and Recreation
NA	Naming Authority
NII	National Information Infrastructure
NIPRNet	SBU Internet Protocol Router Network
NOAA	National Oceanic and Atmospheric Administration
NSA	National Security Agency
NT	New Technology
OCONUS	outside the continental United States
OSD	Office of the Secretary of Defense
PANO	Panograph
PC	personal computer
PDRL	Permanently Disabled Retired List
PHS	Public Health Service
PID	Personal Identification
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PMA	Policy Management Authority
PMO	Program Management Office
PO	Project Officer
POC	point of contact
POS	point of service
POW	Prisoner of War
PPTP	Point-to-Point Tunneling Protocol
RA	Registration Authority
RAPIDS	Real-Time Automated Personnel Identification System
RAS	remote access service
RESRET	Guard/Reserve Retired
ROTC	Reserve Officer Training Corps
RSC	RAPIDS Smart Card
SA	Special Agent
SCI	Sensitive Compartmented Information

SES	Senior Executive Service
SIPRNet	Secret Internet Protocol Router Network
SPD	Separation Program Designator
SPO	Service Project Officer
SSB	Special Separation Benefit, 120 days of entitlement
SSL	Secure Sockets Layer
SSM	Site Security Manager
SSN	Social Security Number
SVGA	Super Video Graphics Array
SVO	Super Verifying Official
TA	Transition Assistance
TAMP	Transition Assistance Management Program
TA-30	Transition Assistance, 30 days of entitlement
TA-60	Transition Assistance, 60 days of entitlement
TA-90	Transition Assistance, 90 days of entitlement
TA-120	Transition Assistance, 120 days of entitlement
TA-RES	Selective Reserves Transition Assistance
TDRL	Temporary Disabled Retired List
TIN	Temporary Identification Number
TSACS	Terminal Server Access Controller System
UIC	Unit Identification Code
UPS	Uninterruptible Power Supply
URFS	Unremarried Former Spouse
URW	Unremarried Widow(er)
US	United States
USA	United States Army
USAF	United States Air Force
USB	Universal Serial Bus
USC	United States Code
USCG	United States Coast Guard
USMC	United States Marine Corps
USN	United States Navy
USS	United Seaman's Service
VO	Verifying Official
VSI	Voluntary Separation Incentive
WAN	wide area network
Y2K	Year 2000

## Appendix F – Privacy Act Statement

The public reporting burden for this collection of information is estimated to average 10 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 this burden, to Department of Defense, Washington Headquarters services, Directorate for Information Operations and Reports (0704-0020), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. 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 OMD control number.

PLEASE DO NOT RETURN YOUR COMPLETED FORM TO THIS ADDRESS.  
RETURN COMPLETED FORM TO THE UNIFORMED SERVICE ID CARD ISSUING FACILITY.

### SECTION VII - PRIVACY ACT STATEMENT

AUTHORITY: 10 U.S.C. sections 1061 - 1065, 1072, 1074, 1074a – 1074c, 1076, 1077, 1095(k)(2), E.O. 9397.

PRINCIPAL PURPOSE(S): To apply for the Uniformed Services Identification card and/or DEERS Enrollment.

ROUTINE USE(S): To appropriate business entities, individual providers of care, and others, on matters relating to claims adjudication, program abuse, utilization review, professional quality assurance, medical peer review, program integrity, third party liability, coordination of benefits, and civil and criminal litigation.

To the Department of Health and Human Services, the Department of Veterans Affairs, the Social Security Administration, and other Federal, state, and local government agencies to identify individuals having benefit eligibility in another plan or program. Applicant information is subject to computer matching within the Department of Defense or with any other Federal or non-Federal agencies. Matching programs are conducted to assure that an individual eligible under a Federal program is not improperly receiving duplicate benefits from another program. A beneficiary or former beneficiary who has applied for privileges of a Federal Benefit Program and has received concurrent assistance under another plan will be subject to adjustment or recovery of any improper payments made or delinquent debts owed.

DISCLOSURE: Voluntary; however, failure to provide information may result in denial of a Uniformed Services Identification Card and/or non-enrollment in the Defense Enrollment Eligibility Reporting System. Failure to provide a beneficiary's Social Security Number renders that beneficiary ineligible for health care services in Military Treatment Facilities. However, emergency health care services will be provided to the extent furnished members of the general public.

### SECTION VIII - CONDITIONS APPLICABLE TO SPONSOR OR APPLICANT

I understand that the actions of the recipient(s) of "Uniformed Services Identification Card" issued as a result of this application are my responsibility insofar as proper use of the card for benefits and privileges authorized; i.e., medical and dental care, exchange, commissary, and morale, welfare, and recreation programs. I will cause the recipient to surrender the card immediately upon call to do so or when appropriate under applicable regulations, and will notify an agency designated to grant authorization for privileges and facilities in event of any change in status affecting a recipient's eligibility therefore.

I am aware that medical care furnished in uniformed services facilities is subject to availability of space, facilities, and the capabilities of the medical staff to provide such care. Determinations made by the medical officer or contract surgeon, or his/her designee, as to availability of space, facilities, and the capabilities of the medical staff shall be conclusive.

Reimbursement shall be required for any unauthorized medical care furnished at government expense. Copies of regulations concerning eligibility requirements are available in the Service Personnel Offices.

By signing this document, the sponsor or applicant certifies that he/she is aware that eligibility for benefits under the Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) terminates for all beneficiaries, except spouses and children of active duty members, and certain disabled beneficiaries under 65, when the beneficiary becomes eligible for Medicare Part A, Hospital Insurance, through the Social Security Administration.

PENALTY FOR PRESENTING FALSE CLAIMS OR MAKING FALSE STATEMENTS IN CONNECTION WITH CLAIMS: FINE OF UP TO \$10,000 OR IMPRISONMENT FOR UP TO FIVE YEARS OR BOTH.

(ACT June 25, 1948, 18 U.S. Code 287, 1001)

## **Appendix G - Procedures for Moving RAPIDS Equipment**

The RAPIDS computer equipment was provided to various military installations in order to automate ID card application preparation and ID card issuance. It presently accesses the DEERS database to update family member and sponsor records so they may receive the benefits to which they are entitled. The categories of systems are defined as in the following paragraphs.

### **RAPIDS Server System**

The server can support directly connected workstations and remote (on-base or cross-town) workstations. The basic RAPIDS server consists of a PC, UPS, a mouse, an Ethernet switch, multi-port connector box, and optional modems (as required). The server system provides security services for its workstations, stores site specific information, such as customized DD Form 1172 settings, stores offline records generated by its workstations (if any), and gathers audit trail information for generating reports at the site level for its workstations. RAPIDS servers can provide communications services, which RAPIDS workstations use to access the DEERS database. The workstations are connected to a server system via modems, direct connections, LANs or WANs.

### **RAPIDS Workstation**

The workstation is the hardware and software that actually produces the various Uniformed Services ID and Privilege cards, Geneva Conventions cards, and select DoD Civilian ID cards and the DD Form 1172 application for Uniformed Services ID and Privilege cards. Sites with smart card production hardware can produce the DoD Smart Card via RAPIDS. Workstations are comprised of a PC, digital camera, laminator, bar code slot scanner/decoder, fingerprint scanner, laserjet printer, surge suppresser and optional modem (if required) connecting the workstation to the RAPIDS server. A workstation may connect to the RAPIDS server via a modem, an Ethernet LAN/WAN connection, a Token Ring LAN/WAN connection, or a simple cable. For auditing purposes, RAPIDS workstations must have access to a RAPIDS server in order to generate an ID card and print a DD Form 1172.

### **Procedures for Moving RAPIDS Equipment**

When an activity finds it necessary to relocate a RAPIDS server system, workstation(s), or both, specific procedures must be followed. The activity must notify the appropriate DEERS/RAPIDS SPO and the D/R Ops Div for CONUS, Alaska, Hawaii, Virgin Islands, Cuba, and Puerto Rico or D/RSC if located in Europe or the Western Pacific Theater, before any relocation will be performed. Any relocation performed by a site without permission from the D/R Ops Div or DRSC is considered an unauthorized relocation. If damage is incurred to the server and/or workstation systems during an unauthorized move, the activity will be responsible to provide funding for all equipment repairs or replacements. Relocation of server equipment requires 120 days notification for coordination purposes. Relocation of remote workstation(s) requires 90 days notification.

The Government contractor will be dispatched to the site to perform the relocation unless a self-help move by the site is specifically approved by the D/R Ops Div. This approval will be based

on the qualifications of people tasked to perform the move and the type of move required. All costs associated with the relocation will be funded by the requesting activity. The following procedures should be followed for a relocation request.

Submit a written request to the D/R Ops Div / DRSC via your DEERS/RAPIDS SPO (see Request Form at the end of this appendix). Complete all information on the Request Form; the form will be returned if incomplete. Your request should reach the DEERS/RAPIDS SPO at least 135 days prior to the requested move date.

Upon approval, the relocation contractor will contact you to determine what services and additional equipment will be required to complete your move.

The D/R Ops Div will determine funding requirements. The D/R Ops Div, the D/RSC (European and Western Pacific sites only), or your DEERS/RAPIDS SPO will notify you of the total funds required for relocation. Local moves may be authorized when qualified technicians are tasked with accomplishing the moves. In these cases, the site command structure assumes responsibility for the move. In such cases, the site will be contacted by telephone to provide instructions and assistance in moving the equipment and connecting it in the new location. If any of the relocated components fail to operate correctly after the move, the site will be responsible for all maintenance and repair costs. Self-help relocations will only be allowed with advance approval from the D/R Ops Div.

The funding documentation should be submitted to the D/R Ops Div. Delivery Orders for a move will not be processed without the necessary funding documents. Funds must be Operations and Maintenance, and procurement will be through direct citation only. Travel funds are not acceptable. The activity's billing office address and POC should be included on the form so that the D/R Ops Div can forward a copy of the delivery order.

**Note:** The only acceptable funding document is the DD Form 448 (Military Interdepartmental Purchase Request [MIPR]). The form must include accounting information and the exact amount to be transmitted. POCs with phone numbers and fax numbers should be included. Send the form to:

Defense Manpower Data Center  
Attn: DEERS/RAPIDS Operations Division  
1555 Wilson Blvd, Suite 609  
Arlington, Virginia 22209-2593

### **Responsibilities of the Designated Installation POC For DEERS/RAPIDS**

Contact your DEERS/RAPIDS SPO by telephone as soon as you are aware of the move.

Contact your Base communications office to determine if they can move the circuit for the server/workstation or if the IP address will change for workstations connected via your LAN. If so, the installation POC shall coordinate the circuit relocation.

Complete the relocation request form and forward it to your DEERS/RAPIDS SPO, who will then forward it to the D/R Ops Div / D/RSC.

After notification by the D/R Ops Div / D/RSC or your DEERS/RAPIDS SPO of approval and the necessary funding, contact your resource management (billing) office for funding documents required (MIPR).

Forward the funding document to the D/R Ops Div. For additional information contact:

**CONUS, Alaska, Hawaii, United States Virgin Islands, Cuba, and Puerto Rico**

Defense Manpower Data Center  
DEERS/RAPIDS Operations Division  
1555 Wilson Blvd, Suite 609  
Arlington, Virginia 22209-2593  
DSN: 426-2000/2001  
Comm: (703) 696-2000/2001  
Fax: (703) 696-1461

**Europe**

DEERS/RAPIDS Support Center – Europe  
HQ, LRMC  
CMR 402, Attn: DRSC-E  
APO AE 09180-3460  
DSN: 486-7365  
Comm: 011-49-6371-921823  
Fax: 011-49-6371-921831

**Western Pacific**

DMDC Support Office (DSO) – Asia/Pacific (Seoul, Korea)  
Comm: 011-822-7914-6195  
DSN: 724-6195  
DSN Fax: 724-6204  
Fax1: 011-822-795-1092  
Fax2: 011-822-7914-6204

**RAPIDS Relocation Cost Estimating Procedures**

The D/R Ops Div has personnel located in the Washington D.C., metropolitan area to perform relocations. All relocation costs will be determined by using estimated labor, travel costs and the cost of any additional equipment required as a result of the move. A workstation that is on the same Base as the server and does not require a modem for communications is referred to as “co-located.” A workstation that is not on the same Base as the server or requires a modem for communication or is connected to the LAN is referred to as “remote.”

The D/R Ops Div also has personnel located in the DRSC-E located in Germany and the DSO-A located in Korea to perform relocations. All relocation costs will be determined by using estimated labor, travel costs, and the cost of any additional equipment required as a result of the move.

**Factors Considered For All Relocations**

**Site Survey.** An on site survey will be required if the relocation contractor determines that the relocation information obtained over the phone does not provide sufficient detail to ensure a successful relocation. These charges will be included in the cost estimate.

**Miscellaneous Charges.** Additional charges will be incurred when it is necessary to purchase and ship additional equipment, i.e., cables or modems, to complete the relocation. These costs will be included in the cost estimate.

**Configuration Changes.** Movement of equipment that causes changes to the system's configuration will generate additional equipment costs, to be determined by the D/R Ops Div during preliminary planning and included in the cost estimate.

**Transportation Charges.** If the relocation requires shipping of any equipment, the site must bear the shipping costs. This includes Base-to-Base relocations. These costs will be included in the cost estimate.

**Note:** If the relocation is a result of a Base closure and the D/R Ops Div initiates a Base-to-Base relocation, the D/R Ops Div will fund the move.

## **RAPIDS Computer Equipment Relocation Request**

The following information is provided in support of the requested RAPIDS location:

1) Full site name, mailing address, and 9-digit ZIP Code:

---

---

---

---

2) Requested move date: \_\_\_\_\_

3) Site Points of Contact

a) Personnel Site POC

i) Primary POC (First, MI, Last): \_\_\_\_\_

ii) Title: \_\_\_\_\_

iii) Alternate POC (First, MI, Last): \_\_\_\_\_

iv) Title: \_\_\_\_\_

v) DSN Number: \_\_\_\_\_

vi) Commercial Number: \_\_\_\_\_

vii) Fax Number: \_\_\_\_\_

b) Base Communications POC

i) POC (First, MI, Last): \_\_\_\_\_

ii) DSN Number: \_\_\_\_\_

iii) Commercial Number: \_\_\_\_\_

4) RAPIDS Equipment being relocated: (Please list all components.)

Server Equipment \_\_\_\_\_

Workstation Equipment \_\_\_\_\_

Additional Equipment \_\_\_\_\_

5) Location of equipment and telecommunications lines:

	<u>Present</u>	<u>Proposed</u>
a) Building Name:	_____	_____
b) Building No:	_____	_____
c) Floor No:	_____	_____
d) Room No:	_____	_____
e) Street Name:	_____	_____
f) Comm No:	_____	_____
g) DSN No:	_____	_____

This information must be provided in order for the communications contractor to move telecommunication lines. Street name should be the name of the street that the building is located on. This is needed even if the building is on base.

6) Network LAN information:

IP address of Server: \_\_\_\_\_

Subnet Mask: \_\_\_\_\_

Default Gateway: \_\_\_\_\_

IP address of Workstation(s) \_\_\_\_\_

\_\_\_\_\_

Subnet Mask: \_\_\_\_\_

Default Gateway: \_\_\_\_\_

Comm (LAN administrator) POC: \_\_\_\_\_

Commercial Phone Number: \_\_\_\_\_

DSN number: \_\_\_\_\_

7) Additional comments and information relative to the relocation:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

## **Appendix H - Site ID Initial Request (DEERS)**

On the following page is a copy of the Site ID Initial Request form. This form should be completed by the SSM and submitted to the appropriate PO when requesting an initial DEERS site ID.

**Note:** All items must be completed on this form. Omission of any items may prevent or delay the processing of this form.

**SITE-ID INITIAL REQUEST (DEERS)**

**SECTION I.** (To be completed by the base/installation/facility RAPIDS Site Security Manager)  
A new site-ID requested for (base name) \_\_\_\_\_

**SERVICE/ORGANIZATION** (Check  One)

Air Force = F _____	Marine Corps = M _____	Public Health _____
Army = A _____	Navy = N _____	Other = X _____
Coast Guard = P _____	NOAA = O _____	
DoD = D _____	OCHAMPUS = C _____	

**TYPE OF FACILITY** (Check  One)

Dental Clinic = D \_\_\_\_\_  
 Health Clinic = M \_\_\_\_\_  
 Hospital = H \_\_\_\_\_  
 \_\_\_\_\_  
 Personnel Office = P \_\_\_\_\_  
 Other = Z \_\_\_\_\_

**FACILITY SECTION** (Check  One)

AAFES = S \_\_\_\_\_  
 AQCESS/CHCS = G \_\_\_\_\_  
 Army Fin Off = F \_\_\_\_\_  
 Civ Person Off = C \_\_\_\_\_  
 Other = Z \_\_\_\_\_

FINCTR w/Title III = FT \_\_\_\_\_  
 Medical/Dental Rec = R \_\_\_\_\_  
 Tumor Registry = T \_\_\_\_\_

OPFAC, PAS, RUC or UIC code is \_\_\_\_\_.

\*See Section II below, EQUIPMENT NOTE.

**SAMPLE**

Chief, Health Services
<b>**REMAINDER OF ADDRESS</b>
USCG Clinic, New Orleans
Attn: Medical Records
4640 Urquhart Street
New Orleans, LA 70017-1010

**FULL MAILING ADDRESS**

Point of Contract (title, not person's name)
REMAINDER OF ADDRESS

\*\*This line of address must include a location identifier.

For example, USCG Clinic is not acceptable. USCG Clinic, New Orleans is acceptable.

Requested by (Rank/Name/Signature) \_\_\_\_\_ DATE: \_\_\_\_\_  
 (Telephone) AVN \_\_\_\_\_ (Comm) \_\_\_\_\_

**SECTION II/III.** (To be completed by SPO)

Recommended by (Rank/Name/Signature) \_\_\_\_\_ DATE: \_\_\_\_\_

**APPLICATIONS** (Check  One)

ACTUR _____	ARED _____	DOLI _____	OLGR _____	RAPIDS _____
AQCESS/CHCS _____	DMRIS _____	GIQD _____	OLPU _____	OTHER _____

**EQUIPMENT** (Check  One) \*NOTE: Justification must be attached if equipment is required.

CRT _____	RAPIDS _____	Telephone Center _____
Facility Equipment _____		Timeshare _____

III. 12-Month Workload: (A) Avg Admissions: \_\_\_\_\_ (B) Avg Outpat Visits: \_\_\_\_\_ (C) Dental: \_\_\_\_\_

**SECTIONS IV/V.** (To be completed by the DEERS/RAPIDS Ops Div.)

V.

DEERS/RAPIDS Operations Division  
 1555 Wilson Boulevard, Suite 609  
 Arlington, Virginia 22209-2593

Inpatient \_\_\_\_\_  
 Outpatient \_\_\_\_\_  
 Dental \_\_\_\_\_

The application(s) above are correct (or changed as indicated), and the equipment is confirmed. Eligibility checking requirements are in Section V. Issue Site-ID.

DATE: \_\_\_\_\_



## Appendix I - QWS3270 Emulator

QWS3270 is a client application, terminal emulator that allows a PC running Windows to connect to an IBM mainframe. The RAPIDS application uses QWS3270 in order to take advantage of the Windows point and click environment.

**Note:** RAPIDS workstations connected to an Active Duty or Air Force Reserve RAPIDS server may not have this application.

A terminal emulation application allows workstations to be used as IBM 3270 type terminals. Workstations must have the ability for use as IBM 3270 type terminals to access the DEERS mainframe-based Eligibility applications such as DEERS Online Inquiry (DOLI) and Panograph (PANO)/Deoxyribonucleic Acid (DNA). Project Officers can also use this to access other Eligibility applications.



Use the following instructions to start the QWS3270 application:

Double-click the QWS3270 Application icon from the desktop.

If your screen does NOT display “Welcome to AHIPC” OR “Welcome to CICS”, select **Connect** from the application main menu. If the “Welcome to AHIPC” screen displays, go to step four. If the “Welcome to CICS” screen displays, go to step five.

A message box indicating the server IP address port and the type of language file will be displayed. If your IP address is 199.209.11.20, click **OK** to advance to the next screen. If your IP address is 199.209.11.14, go to step five.

The “Welcome to AHIPC” screen will be displayed. At the prompt, type **DEERS** and press **ENTER** to enter the DEERS database.

The “Welcome to CICS” screen will be displayed.

Type **LOGN** at the “Welcome to CICS” screen and press **ENTER**.

Accessing the DEERS mainframe can be helpful if a family member is having claims problems or being denied medical care while RAPIDS is reflecting the correct eligibility. The VO can access DOLI to ensure that the RAPIDS eligibility is reflecting in DEERS Eligibility. To view the Eligibility database for verification of dependents, RAPIDS users can access DOLI. Use the following instructions to access the DOLI application.

At the DMDC Security screen, enter your DEERS log on ID and password. Enter **DOLI** at the “Tran ID” prompt and press **ENTER**.

At the DEERS Online Access Main Menu, enter the function 01 for a sponsor inquiry or 02 for dependent inquiry. Next, enter the Sponsor’s Identifier and press **ENTER**.

If you selected a sponsor inquiry, the sponsor's record is displayed. After the user has retrieved the necessary information, press **ENTER** to return to the main menu.

-or-

If you selected a dependent inquiry, the Family Roster screen will appear. Type **V** (for view) in the space where your cursor is displayed. Also type a **V** next to any family member's record you wish to view. Press **ENTER**. The selected dependent records will be displayed. Press **ENTER** to view the next dependent or to return to the main menu when on the last dependent.

At the Main Menu, repeat step two to view another family, or enter **03** in the Function Field to log off.

**Note:** The Default Server field in the Option Setup window indicates the IP address of the TN3270 server at Auburn Hills, Michigan, to which the user is assigned. Users should not always keep the TN3270 application open. The desired information should be viewed and then the user should properly log off by first logging out of the DEERS application, then closing the QWS3270 Emulator.

To view the database for verification of PANO/DNA, users can access the PANO/DNA application. Use the following instructions to access the PANO/DNA application.

On the Security screen enter your DEERS log on ID and password. Enter **PANO** at the "Tran ID" prompt and press **ENTER**.

On the PANO/DNA Inquiry System screen type up to 17 SSNs of panographs/DNA to be checked. Type **PI** (Process Information) in the Action Field and press **ENTER**.

To do additional checks, type **CS** (Clear Screen) in the Action Field and repeat step two.

To sign off, type **SO** in the Action Field.

## Appendix J – Special Character Reference

Character	Name	Location or Action
`	Accent Mark	Top row, next to the “1” key.
~	Tilde	Press Shift + the Accent Mark key.
!	Exclamation Point	Press Shift + the “1” key.
@	At	Press Shift + the “2” key.
#	Number Sign	Press Shift + the “3” key.
\$	Dollar Sign	Press Shift + the “4” key.
%	Percent	Press Shift + the “5” key.
^	Carat	Press Shift + the “6” key.
&	Ampersand	Press Shift + the “7” key.
*	Asterisk	Press Shift + the “8” key.
(	Open Parentheses	Press Shift + the “9” key.
)	Close Parentheses	Press Shift + the “0” key.
-	Dash	Top row, next to the “0” key.
_	Underscore	Press Shift + the Dash key.
=	Equal Sign	Top row, to the left of the Backspace key.
+	Plus Sign	Press Shift + the Equal Sign key.
[	Open Square Bracket	Second row, next to the “P” key.
]	Close Square Bracket	Second row, next to the Open Square Bracket key
{	Open Curly Bracket	Press Shift + the Open Square Bracket key.
}	Close Curly Bracket	Press Shift + the Close Square Bracket key.
\	Back Slash	Second row, above the “Enter” key.
	Pipe	Press Shift + the Back Slash key.
;	Semi-colon	Third row, next to the “L” key.
:	Colon	Press Shift + the Semi-colon key.
‘	Single Quote	Third row, directly left of the “Enter” key.
“	Quotation Mark	Press Shift + the Single Quote key.
,	Comma	Fourth row, next to the “M” key.
.	Period	Fourth row, next to the Comma key.
/	Forward Slash	Fourth row, next to the Shift key.
<	Less Than Sign	Press Shift + the Comma key.
>	Greater Than Sign	Press Shift + the Period key.
?	Question Mark	Press Shift + the Forward Slash key.

## Appendix K – Deployable Hardware Diagrams

### RAPIDS Deployable Hardware Windows 2000 Configuration

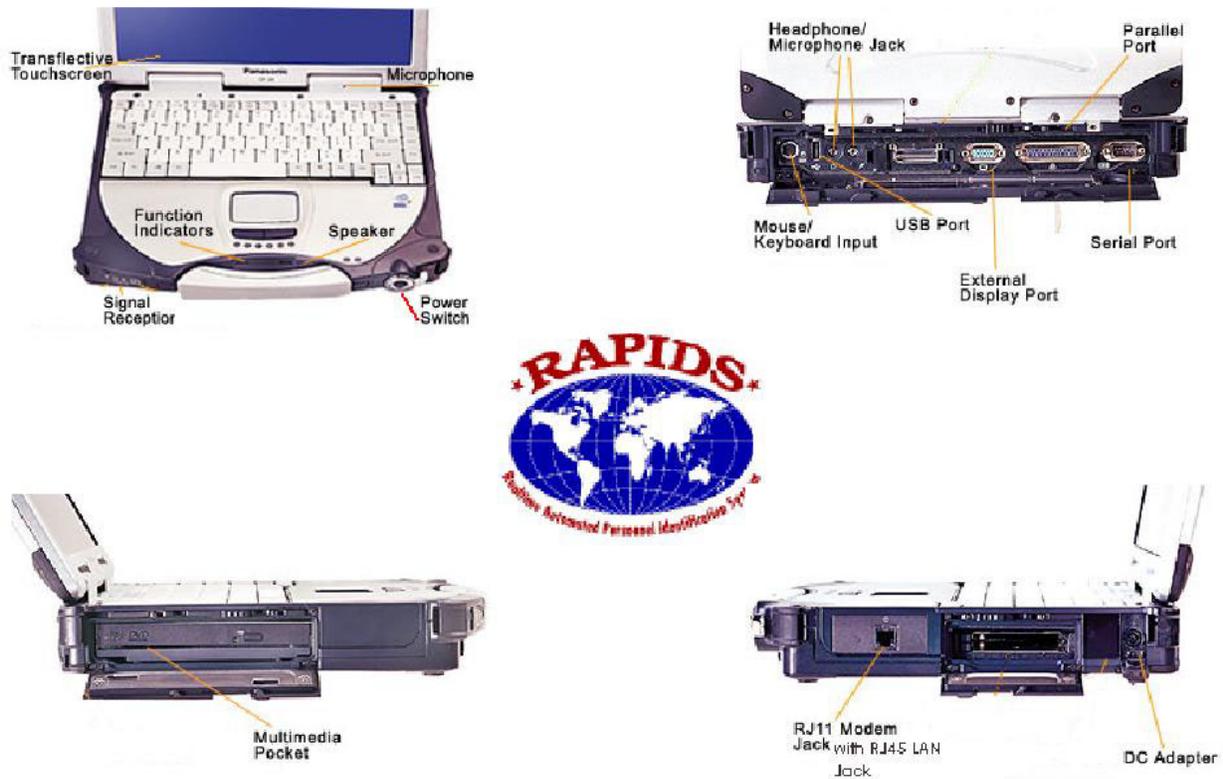
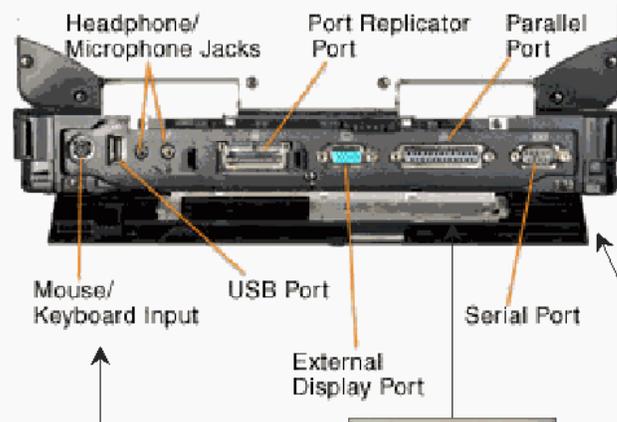


Figure 1. RAPIDS Deployable Hardware

**Mouse and Keypad**

Plug the keypad directly into the PS2 port.

NOTE: Do not use a mouse with these systems.



**FARGO PRO LX**

- 1) Attach Dongle to Parallel Port.
- 2) Attach Pro LX printer cable to the Dongle.
- 3) Plug in AC adapter to back of printer and into surge protector.



**Metro Logic Bar Code Reader**

- 1) Plug connector into serial port.
- 2) Attach AC adapter plug to the serial port connection cable.
- 3) Plug AC adapter into surge protector.

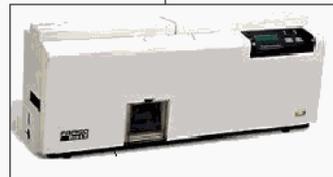
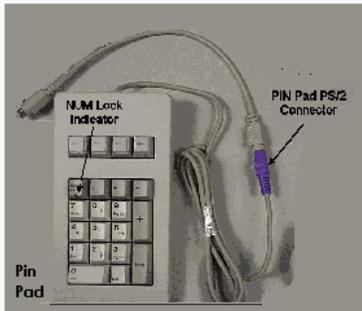
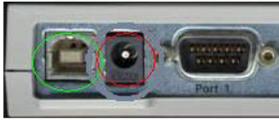
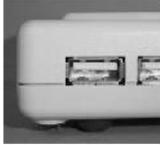


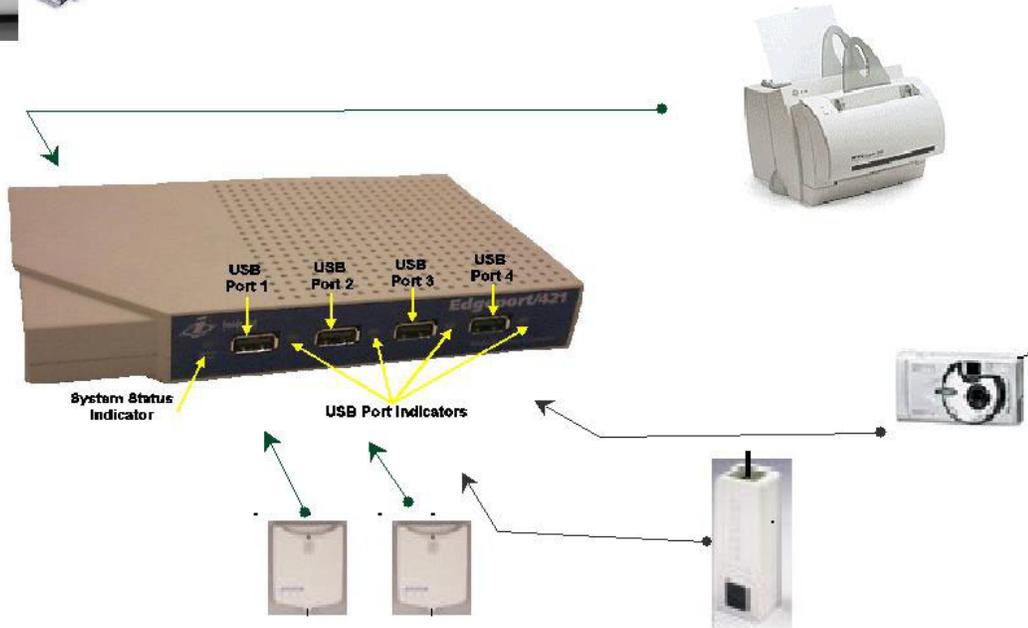
Figure 2. Laptop Peripheral Connections



The back of the hub houses the Type A slot for connection to the laptops USB, the plug in for the AC adapter. Also the are two communication ports and one LPT port. The only device plugged in will be the HP printer.

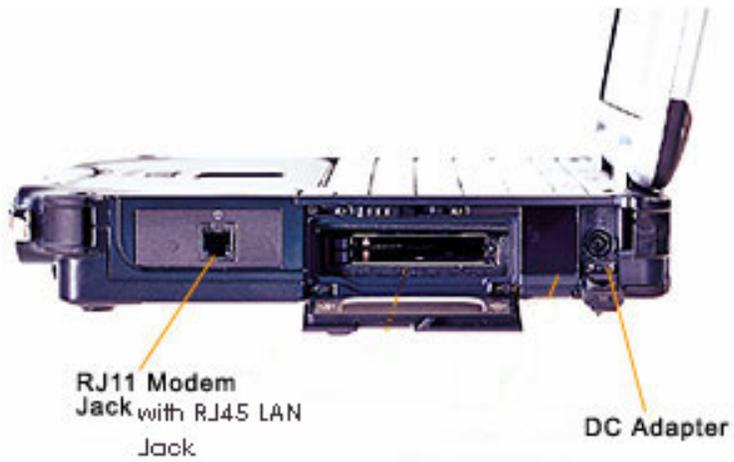


The front of the hub has four USB slots, which will be used to connect the two card readers, fingerprint reader, and camera.



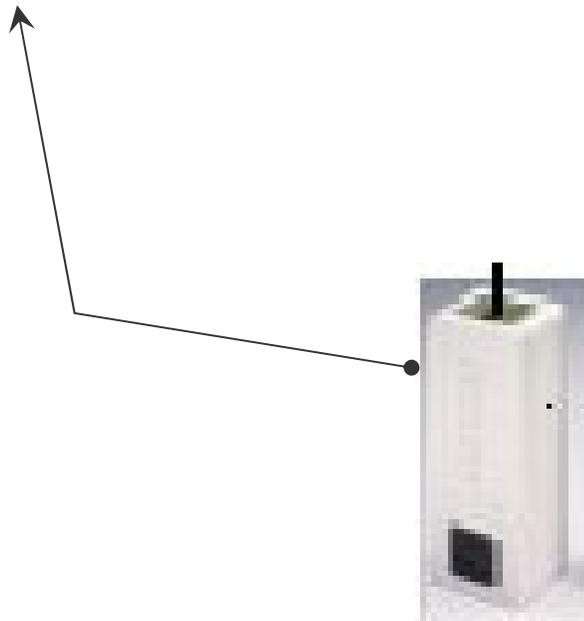
Hook up should be as follows: Port 1= VO Reader, Port 2= Customer Reader, Port 3=Finger print reader, Port 4=Camera

Figure 3. USB Connections



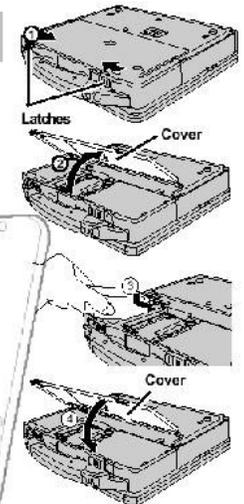
PCMCIA Card slot that houses the MRT Card to connect to the fingerprint reader.

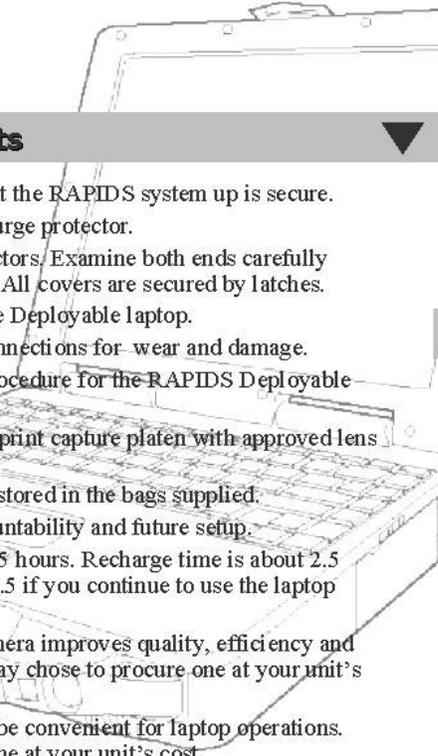
NOTE: Make sure card is in the bottom slot.



**Figure 4. PCMCIA Slot**

### Changing the battery ▶





### Setup and operation hints ▼

- ⌘ Insure that the area you plan to set the RAPIDS system up is secure.
- ⌘ Plug ALL components into the surge protector.
- ⌘ DO NOT force any of the connectors. Examine both ends carefully before attempting to attach them. All covers are secured by latches.
- ⌘ Hand-tighten all connectors to the Deployable laptop.
- ⌘ Regularly examine cables and connections for wear and damage.
- ⌘ Develop a Standard Operating Procedure for the RAPIDS Deployable system.
- ⌘ Clean the camera lens and finger print capture platen with approved lens cleaning cloth only.
- ⌘ Keep all equipment together and stored in the bags supplied.
- ⌘ Label all cables to facilitate accountability and future setup.
- ⌘ The battery will last between 3 – 5 hours. Recharge time is about 2.5 hours if the laptop is turned off, 5.5 if you continue to use the laptop while recharging.
- ⌘ An inexpensive tripod for the camera improves quality, efficiency and safety of the camera. Your site may chose to procure one at your unit's cost.
- ⌘ A standard PS2 type mouse may be convenient for laptop operations. Your site may chose to procure one at your unit's cost.

### LED Lights ▼

	CAPS LOCK
	Active floppy or CDROM drive
	Active Hard Drive
	Battery condition: Orange Charging; Green – Finished; Red - Low
	Power Status: Green – Power On; Flashing – Suspended Mode

Figure 5. Setup and Operation Hints

## Appendix L – Detailed Deployable Packing Instructions

**Purpose:** The instructions have been provided to assist in the packing/unpacking of the Deployable and systems components. If used, they minimize the possibility of damage during transit.

**Components:** The RAPIDS Deployable system is comprised of three soft-sided cases. Although the actual configuration may vary, the following list includes a composite of all possible components with a description of the item and its location within the soft-sided cases. Components are listed in the recommended packing order. The Computer is located in the smallest of the three soft-sided cases.

Case	Item	Description	Location within Case
1	1	Foam block	Lower rear pocket
1	2	Power Cord/AC charger for Computer	Front lower right pocket
1	3	Floppy drive (CD-ROM installed in computer)	Front lower right pocket
1	4	Floppy disk cable for Panasonic CF-28	Front upper left pocket
1	5	AC adapter for Canon Digital Camera	Front lower left pocket
1	6	Rechargeable batteries for Digital Camera	Front lower left pocket
1	7	Canon Battery charger for camera batteries	Front lower left pocket
1	8	Extra Battery for Panasonic CF-28 notebook	Front upper right pocket
1	9	PS/2 Mouse and 'Y' adapter	Front upper right pocket
1	10	Panasonic CF-28 Computer	Upper Foam Tray
1	11	Canon camera with 15' USB data cable	Upper Foam Tray
1	12	RAPIDS Training Guide & Packing Instructions	On top of Computer
2	1	HP 1100 Printer	Main Compartment
2	2	HP 1100 toner cartridge (in nylon bag)	Front, on top of foam block
2	3	Printer data/power cables for HP 1100	Right front pocket
2	4	Dust cover	Right front pocket
2	5	Surge Suppressor	Right front pocket
2	6	Laminator	Back left pocket
2	7	Plastic case for card stock/laminate	Outside zippered pocket
2	8	User documentation	Back pocket
3	1	Fargo Smart Card Printer	Main Compartment
3	2	Activcard smart card reader/writer (User)	Left front pocket
3	3	Activcard smart card reader/writer (VO)	Left front pocket
3	4	Inside Out Networks USB Hub and cables	Front center pocket
3	5	Cherry PIN pad with PS/2 connectors	Front center pocket
3	6	Fingerprint Scanner, cables, and cleaning items	Right front pocket

**If this equipment is transferred to another user organization, call:**

**In CONUS: 1-800-3RAPIDS (DSN 761-6953)**

**In EUROPE: 011-49-6371-92-1823 (DSN 486-7365)**

**In WESTERN PACIFIC: 011-822-7914-6195 (DSN) 724-6195)**

**Packing Instructions:** See the attached diagrams for location of where equipment should be placed.

The following items are contained on the bottom of the first (smaller) Soft-sided Computer Case in the lower front compartment

Case	Item	Description	Location within Case
1	1	Foam block	Lower rear pocket
1	2	Power Cord/AC charger for Computer	Front lower right pocket
1	3	Floppy drive (CD-ROM installed in computer)	Front lower right pocket
1	4	Floppy disk cable for Panasonic CF-28	Front upper left pocket
1	5	AC adapter for Canon Digital Camera	Front lower left pocket
1	6	Rechargeable batteries for Digital Camera	Front lower left pocket
1	7	Canon Battery charger for camera batteries	Front lower left pocket
1	8	Extra Battery for Panasonic CF-28 notebook	Front upper right pocket
1	9	PS/2 Mouse and 'Y' adapter	Front upper right pocket



The following items are contained on the top of the first (smaller) Soft-sided Computer Case.

Case	Item	Description	Location within Case
1	10	Panasonic CF-28 Computer	Upper Foam Tray
1	11	Canon camera with 15' USB data cable	Upper Foam Tray
1	12	RAPIDS Training Guide & Packing Instructions	On top of Computer



The following items are contained in the Second (Larger) Soft-sided Printer Case:

Case	Item	Description	Location within Case
2	1	HP 1100 Printer	Main Compartment
2	2	HP 1100 toner cartridge (in nylon bag)	Front, on top of foam block
2	3	Printer/power cables for HP 1100	Right front pocket
2	4	Dust cover	Right front pocket
2	5	Surge Suppressor	Right front pocket
2	6	Laminator	Back left pocket
2	7	Plastic case for card stock/laminate	Outside zippered pocket
2	8	User documentation	Back pocket



The following items are contained in the Third (Largest) Soft-sided Printer Case:

Case	Item	Description	Location within Case
3	1	Fargo Smart Card Printer	Main Compartment
3	2	Activcard smart card reader/writer (User)	Left front pocket
3	3	Activcard smart card reader/writer (VO)	Left front pocket
3	4	Inside Out Networks USB Hub and cables	Front center pocket
3	5	Cherry PIN pad with PS/2 connectors	Front center pocket
3	6	Fingerprint Scanner, cables, and cleaning items	Right front pocket

