RAPIDS 6.0 TRAINING GUIDE

Revision 1.2

RAPIDS 6.x Training Guide Revision History

Edited By	Date	Draft
Sangeeta Ryan	June 2000	1.0
Various (DRPO, Field Operations, RAPIDS Development, DISA)	July 2000	1.0
Sangeeta Ryan	September 2000	1.1
Various (DRPO, Field Operations, DISA)	April 2001	1.1
Sangeeta Ryan/ Fred Stark	April 2001	1.2

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

What's New in RAPIDS 6.0?

1. The following Common Access Card (CAC) software and hardware have been added.
   - **Public Key Infrastructure (PKI) certificate management**
   - **Java card applications**
   - **Secure Sockets Layer (SSL) client/server**
   - **Smart card encoders/readers**
   - **PVC card printer**
   - **Personal Identification Number (PIN) pad**
   - **Port replicator (Universal Serial Bus [USB] port device)**
   - **Ability to create the teslin card and the CAC**
   - **A recommended task is displayed each time data is changed that should be updated on the sponsor's CAC. RAPIDS can then update the data on the CAC chip.**
   - **A sponsor can be opened for editing by reading a CAC chip.**
   - **A portable database can be created by reading CAC chips.**
2. Fingerprint matching
   - **Verifying Official (VO) verification: the VO's fingerprint must match the fingerprint in DEERS at application startup.**
   - **The card recipient's fingerprint must match the fingerprint previously stored in DEERS when receiving a CAC.**
   - **If no fingerprint exists in DEERS, one will be captured.**
   - **If a fingerprint in DEERS is an old format, a new one will be captured.**
   - **A VO can choose to override the fingerprint match if three attempts to match a recipient's fingerprint are unsuccessful.**
   - **All decisions by a VO to override a failed fingerprint match are audited.**
   - **When changing a PIN, a fingerprint match or previous PIN must be provided.**
3. RAPIDS searches DEERS for the existence of the person identifier specified when attempting to add a family member or when changing the identifier of an existing family member.
4. Test Identification Number is no longer an option for Person Identifier.
5. RAPIDS possesses the ability to display multiple Messages of the Day with the current message showing first.
6. Many error messages are now more descriptive.

7. Address View/Navigators

   - **Former spouses and deceased or terminated individuals are not displayed in the family selection list.**
   - **RAPIDS automatically sets the country to United States for APO/FPO addresses.**
   - **A field for home e-mail address has been added.**

8. Person Views/Navigators

   - **Default Medicare (eligible at age 65) is now displayed.**
   - **Edits for gender changes will occur just prior to saving to DEERS instead of within a navigator or person window.**
   - **A check box for "Unknown" has been added to the End Date for Base Privilege Suspensions.**

9. Sponsor Views/Navigators

   - **A Civilian Identification Number (CIN) may be used in place of an SSN for DoD and other government contractors that refuse to provide a SSN.**
   - **Changes to the Country of Origin for Foreign Military are allowed.**
   - **Changes to the Geneva Conventions category from "None" to the proper category for Civilians are now allowed.**
   - **Reserve Component Category Code Begin Date is captured and the Reserve Component Category Code can be changed.**
   - **Navy Reserve teslin cards for midshipmen at United States Merchant Marine Academy, Kings Point, New York, may now be issued.**
   - **Fields for e-mail addresses have been added to the Sponsor's Service record view.**

10. Dependent Views/Navigators

   - **A choice of "adoption" has been added to the list of termination reasons for children, stepchildren, and wards.**
   - **The Relationship Condition of Court Order has been changed to "Court Order/Pre-adopt."**
   - **If a sponsor has a Foreign Identification Number (FIN), and the family member is added with the "None" box selected for Person Identifier, the DEERS database will assign a FIN to the family member.**
   - **Users have the option to enter a specific end date for the relationship of Ward.**
   - **The Verify screen will no longer display deceased or terminated family members.**
   - **The eligibility end date for children, stepchildren, and wards, as shown on the Benefits View, will display as the day before the family member's twenty-first birthday.**

11. Personnel Data and Condition Changes

   - **RAPIDS will calculate the end date for Personnel Conditions if the number of duty days is entered.**
   - **Changes to Agency/Subagency for DoD civilians are allowed.**

- **Reserve Retired sponsors may now be terminated.**
- **Special Operation conditions that are less than 30 days are now allowed.**
- **Edits have been made to allow for sponsors to be 16 years of age.**
- **When Date of Death is changed, RAPIDS will automatically change the end dates of any segments that are terminated due to death.**
- **Only users with the DMDC Support Office (DSO) or Project Officer (PO) role may perform an Invalid Entry Transaction (IET) on Service-verified Personnel Categories and Conditions.**

12. Verification, Identification (ID) Card, and DD Form 1172 Changes

- **Next verification date for Former Spouses will be set to "Unknown."**
- **When creating a new card, the date at which the previous ID card should be marked as terminated can now be entered.**
- **The correct status is shown on the front of the ID card for Former Member DD Form 2RRT card.**
- **When Medicare is terminated, RAPIDS will remove it from the DD Form 1172.**
- **The Direct Care field on the DD Form 1172 for DoD Contractors has been corrected to reflect "X" benefits.**
- **Deceased and terminated family members will not be displayed on the DD Form 1172 Navigator list.**
- **Once a family is opened and an ID card created, the VO cannot terminate the card without reopening from DEERS.**
- **The dependent of a sponsor in Prisoner or Appellate leave status will show Active Duty as the sponsor's status on his/her DD Form 1173.**

13. Communications

- **SSL has been added for communications between the workstation and DEERS.**
- **Updates have been made to the transaction process to confirm that audits are successful. Some transactions made were not previously recorded on the reports.**
- **The start of offline record processing will be staggered when the entire system has been down. All offline uploads from all servers previously occurred at every hour and half-hour. Now each server will have a random point within the half-hour to begin the upload process.**
- **If RAPIDS is unable to communicate with DEERS after double-clicking on the "Offline" tag in the status bar, the reason for the failure is displayed.**
- **Performance and reliability have been improved for systems that rely on their authentication server to determine the DEERS communication status.**

14. Hardware Devices

- **RAPIDS supports the Kodak DC280 camera for deployable systems.**
- **The fingerprint capture area has been changed to improve digitized fingerprint quality.**

- **Matrox Meteor framegrabber cards can now be auto-tuned for optimal fingerprint quality.**
- **RAPIDS workstation supports the following CAC peripherals: two smart card encoders/readers, PVC card printer, and PIN pad.**
- **The RAPIDS server supports a smart card encoder/reader.**
- **RAPIDS now has an external bus for connecting peripherals, the USB port device, that transfers data at high speeds.**

15. The following Hot Keys have been updated.

RAPIDS View	Hot Keys
Address View	CTRL+A
Benefits View	CTRL+B
Copy	CTRL+C
DD Form 1172 View	CTRL+D
Characteristics View	CTRL+H
ID Card View	CTRL+I
New Family	CTRL+N
Open from…	CTRL+O
Insurance View	CTRL+P
Service Record	CTRL+R
Save	CTRL+S
Save Family	CTRL+SHIFT+S
Paste	CTRL+V
Undo	ALT+BACK
Cut	SHIFT+DELETE
Help	F1
Help\Context	SHIFT+F1
Open Offline	F10
Open Mass Issue	F11
Add Dependent	F2
Update Address	F3
Create DD Form 1172	F4
Reopen Family	F5
Next Pane	F6
Previous Pane	SHIFT+F6
Create ID Card	F7
Verify Dependents	F8
Open	F9
Family Tabs (toggle on/off)	ALT+X
Family Tree (toggle on/off)	ALT+Z
Switch Tabs within a View	CTRL+PGUP CTRL+PGDN
Activate the Control	ALT+Underlined Letter
Close Current Window	CTRL+F4
Switch Between Views	CTRL+TAB CTRL+SHIFT+TAB CTRL+F6 CTRL+SHIFT+F6

Table of Contents

1 Overview

1.1 Introduction

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 Program Office (D/RPO) 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 Common Access Card (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. The purpose of the RAPIDS Training Guide is to provide a written guide for Field Service Representatives (FSRs) to use during initial training at RAPIDS sites and for RAPIDS users to reference when new personnel are assigned into a personnel office

1.2 What Are the Functions 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 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.

1.3 What Are the Objectives Of the RAPIDS Training Guide?

The following are the four main objectives of the RAPIDS Training Guide.

1. To provide a basic knowledge of the DEERS database, its communications network, and its interaction with RAPIDS.
2. To allow users to function comfortably in the Windows environment.
3. To allow users to utilize the RAPIDS application, print a DD Form 1172, and issue the automated ID card and CAC without assistance.
4. To use this Training Guide to instruct new users of RAPIDS.

1.4 Where Do I Go For Help with Regulations?

The Interservice Publication, AFI 36-3026, "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://afpubs.hq.af.mil. The Interservice Publication is listed as AFI 36-3026. 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

The Air Force maintains an informative and helpful web site for DEERS and RAPIDS issues. Go to www.afpc.randolph.af.mil/deers and view numerous policy topics, helpful tips and links to other 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 Verifying Officers (VOs) interpret the proper answers to their policy issues.

2 Explaining DEERS and RAPIDS

2.1 Introduction

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, Geneva Conventions, DoD Civilian ID cards, or CACs.

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 6.0 was developed to include the hardware, software, communications, and security requirements to issue the CAC.

2.2 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.

2.3 What is the 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 and print the DD Form 1172. 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.

2.4 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.

2.5 What is 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 3* of this Training Guide.

3 Infrastructure

3.1 RAPIDS Components

Physically, RAPIDS consists of servers and workstations located throughout the continental United States (CONUS), Alaska, Hawaii, United States Virgin Islands, Cuba, Puerto Rico, throughout Europe, and throughout the Western Pacific theater. As previously mentioned, RAPIDS workstations and servers communicate with the DEERS database using the DII. Outside of RAPIDS, a telecommunications infrastructure and systems architecture is necessary to support the CAC. The architecture, which includes the Issuance Portal and Certificate Authorities (CA) consists of several systems working together.

1. DEERS database
2. RAPIDS server
3. RAPIDS workstation
4. Defense Information Systems Network (DISN) / Nonclassified but Sensitive Internet Protocol Router Network (NIPRNet)
5. Issuance Portals
6. PKI CA

3.1.1 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.

3.1.2 Server

The RAPIDS server consists of a personal computer, Uninterruptible Power Supply (UPS), an Ethernet switch, a multiport connector box, optional modems (as required), a surge suppressor, and, in some instances, a laser printer.

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 local area network (LAN), or a wide area network (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.

3.1.3 Workstation

The workstation component is the hardware and software that actually produces the ID card, the CAC, and the DD Form 1172 or 1172-2. Workstations are usually comprised of 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 o r r r .

A workstation may connect to the RAPIDS server via a modem, a LAN/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. RAPIDS workstations require connection to the Issuance Portal and CA to produce the CAC.

Note: 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. The digital camera is shipped with a remote control unit. This remote is not needed when using the RAPIDS application. The remote should be stored in a safe place for future use.

3.2 What is the 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 a sub-element of the DI). 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. DISA is centrally operating at least two worldwide Internet protocol (IP) router networks, one for the sensitive but unclassified (N) environment, NIPRNet, and one for the secret (S) environment, Secure Internet Protocol Router Network (SIPRNet). 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.

3.3 What is an Issuance Portal?

The Issuance Portal consists of a Web server and Hub broker. The Hub broker serves as a card manager, PIN manager, applet manager, and key manager. This is all done outside of the RAPIDS application. The Hardware Security Module (HSM) is a hardware device used to securely store Master Keys and algorithm pairs. The HSM generates the key pair for e-mail encryption certificates.

3.4 What is a Certification Authority?

The DoD CAs are computer servers 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 and is automated by the CA. The Secure Sockets Layer (SSL) session encrypts all communications between DEERS, RAPIDS, and the CA. Public and private keys help ensure that the information transmitted between computers is secure.

The following 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.

3.5 What Information is Stored in DEERS, on RAPIDS Servers, and on RAPIDS Workstations?

3.5.1 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)

3.5.2 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

3.5.3 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)

3.6 RAPIDS Platform and Programming Languages

RAPIDS servers and workstations use the Windows NT 4.0 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, CICS, Aion DS knowledge base programming (artificial intelligence), C coding, and an Oracle database that resides on a Sun server at the AHSMC.

3.7 CAC Architecture

The CAC differs from the standard Uniformed Services ID card in the following ways. The CAC can be 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 and magnetic stripes, 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 chip 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 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 Digital Signature private keys never leave the card. The E-mail Encryption private keys are generated off the card and escrowed by the CA. It is important for both the CAC recipient and the VO to understand the importance of updating RAPIDS with the correct e-mail address. The correct e-mail address embodies 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.

3.7.1 New RAPIDS Architecture

Under previous versions of the RAPIDS application, the RAPIDS workstation communicated with DEERS via socket-to-socket communications. 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 6.0, RAPIDS achieves Federal Information Processing Standard Level 2 Compliance.

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/Hub.

Some users of RAPIDS 6.0 may notice that additional time is required to issue the CAC in comparison to issuing the teslin cards. The increased level of security and the additional coordination between systems account for this additional time.

The Smart Card Interface provides the RAPIDS core application an intermediary to use the facilities provided by the Hub. This buffers RAPIDS from having to handle security keys, which would make the system more vulnerable to attacks.

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

- Two smart card o r r r - one for the VO to log in and one to encode the ICC during CAC issuance.
- PVC card printer - to print the CAC
- PIN pad - for the CAC recipient to enter his/her private PIN
- USB port device – to provide additional ports to connect the CAC-production peripherals to the RAPIDS workstation.

The RAPIDS server will also receive a smart card encoder/reader to allow the RAPIDS SSM to log in to the server directly for performing administrative duties, such as user administration.

3.8 Public Key Infrastructure

A PKI consists of protocols, services, and standards supporting applications of public key cryptography. The DoD PKI is a system of CAs, Registration Authorities (RAs), directories, client applications, and servers that model trust and allow 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 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 their public key is used by the recipient to verify the signature. When sending an encrypted message, the recipient's public key is used by the sender 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 the 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 easily be detected.

The CA issues each person or entity (such as a server or individual) one or more certificates, which are digital records that contain information, such as the entity's name and public key and the signer's signature and data. Each CAC will contain up to three kinds of private keys for each cardholder, an identity key, email encryption key, and email digital signature key. 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 review 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, therefore, imperative that each individual secures their CAC and does not share or write down the PIN protecting it.

3.9 PKI, the CAC, and RAPIDS

In his 10 November 1999 memorandum, Dr. John Hamre directed all DoD components to take necessary actions to implement the use of smart cards and PKI technology. It was decided that RAPIDS would be the system to produce the new DoD ID card, CAC, which utilizes this smart card and PKI technology. RAPIDS already has the hardware and card management infrastructure to complete this task, thus ensuring full and consistent use of existing capabilities. For the DoD PKI, the RAPIDS workstation fills the roles of the Local Registration Authority (LRA) / RA. The LRA role is encompassed within the RAPIDS VO, Super Verifying Official (SVO), and/or Site Security Manager (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 will employ 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 6.0, 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 6.0 is one of the first DoD PKI enabled application to be implemented worldwide. The VO is required to insert his/her CAC into a smart card encoder/reader attached to the RAPIDS workstation to log in. Windows NT reads the login ID from the CAC. Under the CAC configuration, the workstation will be establishing an SSL session using the VO's PKI identity certificate and key pair. The VO then enters his/her PIN on the workstation's keyboard and places his/her right index finger on the RAPIDS fingerprint scanner for verification to complete the login process. The CAC must remain inserted at all times while using the RAPIDS workstation.

With a few exceptions, all the members of these target populations will be 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.
- Designated DoD contractors who require an electronic card to gain physical access to controlled areas or logical access to Government computers
- Presidential Appointees

The following populations will 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.

The following other populations will continue to 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.

Member Category *(Personnel Category Code)*	**CAC** *(ICC/Non-ICC)*	**Teslin Card** *(Form)*
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	**2RES**
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	**2RES**
Presidential Appointee (B)	**ICC**	*2750/2764*
DoD civil service – requiring electronic access, are emergency essential, or are serving overseas (C)	**ICC**	*2765/2764/2750*
DoD civil service – not requiring electronic access (C)	**Non-ICC**	**N/A**
Lighthouse service (L)	N/A	**2765**
American Red Cross (M)	**N/A**	**2765**
Other Government Agency (non-DoD) - Civil Service (O)	**Non-ICC**	*2765/2764*
Foreign military (T)	**ICC**	*1173/1173-1*
Foreign national employee (U)	**ICC**	*1173*

Member Category *(Personnel Category Code)*	**CAC** *(ICC/Non-ICC)*	**Teslin Card** *(Form)*
DoD contractor – designated (E)	**ICC**	*2765/2764*
DoD contractor – not designated, but emergency essential or overseas (E)	***ICC***	**N/A**
Retired (R)	N/A	**2RET**
Reserve retiree (Q)	N/A	**2RESRET**
100% disabled American veteran (D)	N/A	**2765**
Former member - a 20-year active-duty serviceman who was eligible to retire but elected discharge (F)	N/A	**2765**
Transitional Assistance Management Program (F)	N/A	**2765**
Medal of Honor (H)	N/A	**2765**
Family Members – except children under 10	N/A	**1173**
Family Members – designated children under 10	N/A	**1173**

3.10 DEERS/RAPIDS Roles

The following information is discussed in this section.

1. What is a DEERS site ID?
2. What is a DEERS login ID?
3. What is a VO/LRA?
4. What is an SVO?
5. What is an SSM?
6. What is a Service Project Officer (SPO)?
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.

3.10.1 What is a 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/RPO also use a DEERS site ID to generate transaction reports by site. An example of a DEERS site ID is **102333**.

3.10.2 What is a DEERS Login ID?

Every user must have a valid CAC with associated PIN and a DEERS login ID with associated password to sign on to 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 NT login account with a DEERS ID and password for each RAPIDS user at the site. See *Section 5* of this Training Guide for detailed procedures. Initially, your DEERS login ID and DEERS password are distributed to you by mail, ensuring that no one else knows your DEERS password, including the SVO and RAPIDS SSM. The login process lets the system know the users are authorized to use the application. All users must request a unique DEERS login ID from their DEERS SSM. For security purposes, neither the password nor the PIN should be shared with anyone, including other VOs, the SVO, or the RAPIDS SSM. A VO should not sign on to the RAPIDS workstation and allow another person to make updates. The VO should never leave his/her VO CAC unattended in the RAPIDS VO reader.

3.10.3 What is a VO?

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 (provided by the individual application for Uniformed Services Identification Card and DEERS Enrollment) and prints the DD Form 1172-2, (Application for DoD Common Access Card, DEERS Enrollment). The DD Form 1172-2 will **NOT** be prefilled with sponsor information.

3. Generates the PVC CAC smart cards 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 SPO 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.
- 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.
- Provide the CAC recipient with and obtain his/her signature on the Subscriber Certificate Acceptance and Acknowledgement of Responsibilities forms (future enhancement).
- Request that CAC recipients enter the PIN for their CAC.
- Print the CAC.
- Securely communicate requests to and responses from the CA.
- Save applications, certificates, and data to the chip.
- Update the CAC as necessary to reflect any change in the personnel category of the CAC recipient. This automatically issues/revokes certificates as needed.
- Update other data stored on the CAC chip.
- 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.
- Ensure that users understand their responsibilities with respect to the CAC and the information, including the PKI keys and certificates stored on it.

A VO on the RAPIDS system can be any person, military or Government employee. In addition, 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.

3.10.4 What is an SVO?

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 SPO or DSO when a purge, invalid entry, or lock to a record is necessary.

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.

3.10.5 What is an SSM?

The DEERS SSM is responsible for activating all RAPIDS users and assigning roles for new and existing users. They are also responsible for requesting a login ID for a new user via the RAPIDS application and ensuring that new CACs are updated with LRA privileges via RAPIDS. Because of the nature of the position, an SSM should be familiar with the RAPIDS application and user security procedures. The RAPIDS SSM is routinely an SVO as well.

With the addition of the CAC to the login procedure, it becomes more important than ever to ensure an overlap period exists between the out-processing and in-coming RAPIDS SSM. The out-processing SSM should issue a CAC to the in-coming 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 encoder/reader and updating the new SSM as an LRA. 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. This role cannot be added without the assistance of DEERS/RAPIDS Security personnel.

If no overlap occurs between the SSMs, another VO may issue a CAC to the incoming SSM. It will still be necessary to coordinate with DEERS/RAPIDS Security to add the SSM role and for the SSM to be added to the Directory at the DISA Certificate Authority.

With the implementation of RAPIDS Version 6, only RAPIDS SSMs and users signed on with administrator privileges will have RAPIDS server login privileges. Users with assigned roles as VOs and SVOs will no longer be able to log in to RAPIDS servers unless they also have SSM or Administrator privileges. This restriction applies only to servers, not to workstations. The RAPIDS SSM performs the following tasks:

1. Maintains system security by adding and assigning roles for VOs, read-only users, address updating users, and SVOs.
2. Requests new DEERS login IDs and issues VO and SVO CACs.
3. Deletes DEERS login IDs.
4. Resets users' passwords and/or PINS.
5. Administers the offline records generated by the VOs and SVOs at their site, including:

- **Viewing transaction errors.**
- **Monitoring the offline records made by other VOs.**

6. Updates the security privileges on a previously issued DEERS login ID.
7. Views or updates RAPIDS Configuration Utilities found in *Section 9*.

8. Notifies the SPO or DSO when a purge, invalid entry, or lock to a record is necessary.
9. Ensures a Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA) is established between the server and the remote site(s). When there is a change in users, new users must be aware of and agree to the MOU or MOA.
10. Trains new VOs and SVOs on the RAPIDS software using this Training Guide.
11. Ensures that all VOs and SVOs have read and understand the “Message of the Day.”
12. Downloads and installs new RAPIDS software, as instructed.

3.10.6 What is an SPO?

Each Uniformed Service and its Guard and Reserve components have an assigned SPO. The DEERS/RAPIDS SPOs are responsible for service specific 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 SPOs can be found in Appendices **C** and **D** of this guide. An SPO 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/RPO.
6. Provide policy guidance to their RAPIDS users.

3.11 What is the PKI Role of the RAPIDS Workstation?

The RAPIDS workstation serves as the tool used to approve and issue VO certificates on the CAC and revoke certificates as necessary. RAPIDS acts as an “electronic RA.” The DoD PKI will use RAPIDS workstations as RAs, in order 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 1172-2 requests that card recipients identify the country to which they are assigned.

6. The Agency/Subagency for a DoD civilian or DoD contractor is collected.

Note: The RAPIDS 6.0 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 SPO for guidance.

3.12 What are the Responsibilities of the Card Recipient with Respect to PKI?

The CAC cardholder will automatically be issued the appropriate PKI keys and certificates on the CAC with PKI-enabled applications to provide identification, encryption and decryption of documents, and other messages transmitted between computer systems, and for building access.

The following are the responsibilities of the CAC cardholder.

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.

3.13 Where Do I Go for Help if I Have Questions about RAPIDS?

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

1. **RAPIDS Online Help**

2. **D/RAC, D/RSC-E, or DSO-A, based on your site's location.**

3. **DEERS/RAPIDS FSRs**

4. **Your SPO**

5. RAPIDS 6.0 Training Guide on CD-ROM
6. RAPIDS Version 6 Hardware Guide on CD-ROM
7. RAPIDS Version 6 Self-Help Relocation Guide on CD-ROM
8. Security Standard Operating Procedure for RAPIDS
9. Joint Service Publication AFI 36-3026

3.13.1 RAPIDS Online Help

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

Online Help can be found directly in your system while you work with RAPIDS. It was designed exactly like Online Help for Windows to make access quick and convenient. Detailed instructions on how to use Online Help are found in *Section 5* of this Training Guide.

3.13.2 RAPIDS Documentation

Your site has been provided a CD-ROM with the following guides to assist you with the operation of your RAPIDS workstation hardware and software application: RAPIDS 6.0 Training Guide, RAPIDS Version 6 Hardware Guide on CD-ROM, RAPIDS Version 6 Self-Help Relocation Guide, and Security Standard Operating Procedure for RAPIDS. In addition, for RAPIDS policy questions, the Joint Service Publication AFI 36-3026 can be found at the web site listed in *Section 1.4* of this Training Guide. These, along with the RAPIDS online Help should be your first sources for answering questions pertaining to RAPIDS.

3.13.3 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.

3.13.4 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 / DSO-A. FSRs are assigned regionally and assist the users with applications and onsite training. As explained in *Section 1*, your FSR is available to assist you in initial training for the RAPIDS application and follow-up questions. A copy of the most current FSR Regional Map can be found in **Appendix B** of this Training Guide.

3.13.5 Service Project Officers

Each Service has a designated DEERS/RAPIDS Personnel and Medical SPO who can answer any policy questions that you cannon answer by using the Joint Service Publication AFI 36-3026. All requests for new DEERS site IDs, new user login IDs, RAPIDS equipment relocations, additional RAPIDS workstations, and new RAPIDS site equipment should be directed to your Personnel SPO. A listing of SPOs by Service, with phone numbers and addresses can be found in **Appendix C** (Personnel SPOs) and **Appendix D** (Medical SPOs) of this Training Guide.

3.14 What are the 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.

3.14.1 Server Site

The following are responsibilities of the server site.

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/login 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 computer system 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.

3.14.2 Remote Site Responsibilities

The following are the responsibilities of the remote sites.

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.

3.15 When Do I Contact the D/RAC / D/RSC-E / DSO-A and When Do I Contact My Server Site?

Contact the D/RAC / D/RSC-E / DSO-A 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. Records requiring an Invalid Entry Transaction (IET): The site can also contact the DSO, SPO, or FSR for assistance with IET.

5. 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 local area network (LAN), local firewall configuration, wide area network (WAN) or within the DMDC network enterprise. D/RAC / D/RSC-E / DSO-A personnel will work with Defense Information Systems Network (DISN) and local Base communications personnel to resolve all communications issues.

6. 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.

7. 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 M** of this Training Guide.

Contact the serversite with an y of the following concerns.

1. Slow or no communications with the RAPIDS server

2. Modems do not connect

Remote sites should inform their RAPIDS server site of non-hardware related problems first. If the server site cannot assist in resolving the problem, then contact the D/RAC / D/RSC-E / DSO-A.

4 Orientation to Windows NT 4.0

4.1 Introduction

Current versions of RAPIDS are designed for a Windows environment. Windows NT 4.0 (new technology) is an industrial strength operating system. RAPIDS has incorporated the many recent advances in PC technology that provide for more user-friendliness. Some of these user-friendly features include:

1. Users can control certain aspects of how the application looks on their screen.
2. Online Help with step-by-step instructions for common data processing scenarios.
3. Easy to learn and easy to use commands that are spelled out in plain language, which users can choose from menus by clicking the mouse pointer on a button.
4. Pre-sequenced dialogs called “Navigators,” which step the user through many complex transactions, making them much simpler.
5. Onscreen display of DD Forms 1172, ID cards, and CACs, which allows the user to review them for accuracy before printing them.

Important Note: A directive from the D/RPO and SPOs states that sites are not to load any additional software on their RAPIDS servers or workstations at this time. RAPIDS users should not install or activate screen savers (Windows NT or other software) on their RAPIDS systems.

4.2 The Mouse

The basic technique is to turn the mouse so that its cable extends away from the user. The user should place his/her hand over the mouse in such a way that the part of the mouse nearest fits comfortably in the palm of the hand. Also, the user’s index and middle fingers should rest lightly on the two mouse buttons, while the thumb and ring finger hold the mouse on either side. The user are now ready to see the mouse in action. Move the mouse around, and notice that the mouse pointer on the screen moves in the same direction as the mouse itself.

The mouse can perform the following actions:

1. Point means the user moves the mouse so that its pointer rests on a specific screen location.
2. Click means the user quickly presses and releases the left mouse button.
3. Double-click means the user presses and releases the left mouse button twice quickly.
4. A right-click is similar to a regular click, except the user quickly presses and releases the right mouse button.

5. Dragging means the user points the mouse pointer at a particular object, presses and holds down the left mouse button, and then moves the mouse before releasing the mouse button.

4.3 The Keyboard

Although a majority of the user’s movement throughout Windows is made by means of the mouse, the keyboard can be used throughout the RAPIDS application as well. The following are a few of the keyboard’s parts and their relation to Windows.

1. ALT moves the cursor to the menus at the top of the current window.
2. The Numeric Keypad serves two functions. When NUM LOCK is on the user can use the numeric keypad to enter numbers. If NUM LOCK is turned off, the keys can be used to move around the screen without use of the mouse.
3. ARROWS move the cursor around the screen without use of the mouse. In addition to the arrow keys on the numeric keypad, a dedicated set of four arrow keys are located to the left of the numeric keypad on the keyboard.
4. BACKSPACE deletes the character to the left of the cursor. It also deletes all highlighted information.
5. CAPS LOCK works as it does on a typewriter, except that it only affects the letter keys; it has no effect on punctuation symbols or numbers.
6. When using a key in conjunction with another key, this is called a combination. CTRL is used in almost every key combination. For example, holding down CTRL while pressing ESC allows the user to view the options on the Start menu.
7. DELETE removes the character to the right of the cursor. It also deletes all highlighted information.
8. ENTER is basically the same as RETURN on a typewriter. The only exception is that ENTER does not need to be pressed at the end of each row. A word processor can sense when it comes to the end of a line and automatically wraps to the next line.
9. END is used to put the cursor at the end of a line of text.
10. ESC, in general, is used if the user has ended up in an unfamiliar program or screen. The user can usually get back to more familiar “turf” by pressing ESC.
11. PAGE UP/PAGE DOWN allows the user to either advance up or down one page at a time.
12. SHIFT creates uppercase letters, as well as prints the symbols that are above other symbols and numbers on the keyboard when it is held down in combination with those keys.

13. TAB is used to space over an amount of space equal to the tab stops for word processors. TAB can also be used to jump from one box to the next when filling out a form or move the user forward through options in a dialog box.

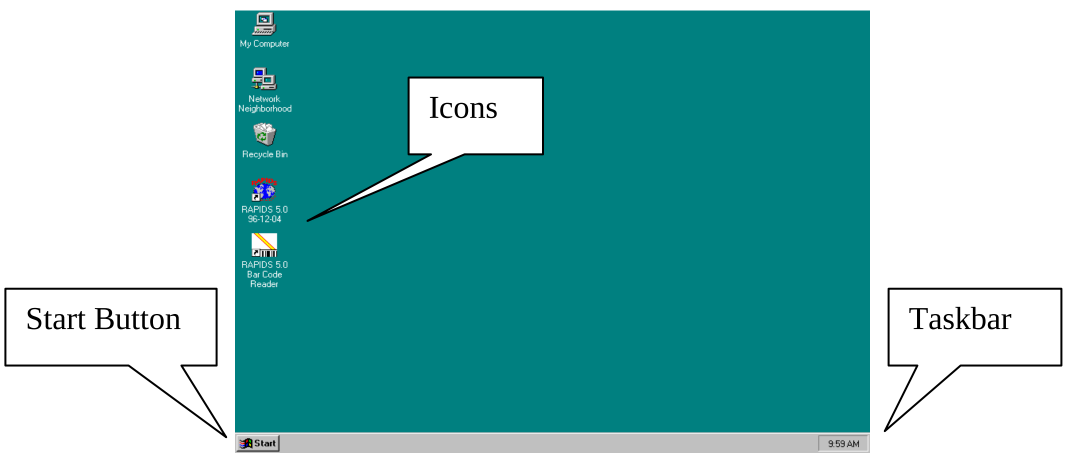
14. The SHIFT+TAB combination moves the user backward through options when in a dialog box.

15. The CTRL+TAB combination moves the user forward through tabs in a dialog box.

4.4 Starting Windows NT 4.0

Once Windows NT 4.0 is installed, it will start itself automatically each time the user turns on the computer. To begin logging on to Windows NT 4.0, the user will be prompted to press the CTRL+ALT+DELETE combination to log in. The Privacy Act Statement will appear stating "Authorized Users Only." The login screen then appears. Refer to *Section 5* of this Training Guide for RAPIDS login procedures. After a successful login, the Windows NT 4.0 desktop appears.

4.5 The Desktop



Windows NT 4.0 Desktop

When the user starts Windows, the large area he/she sees on the screen is called the Desktop. Adding shortcut icons or adjusting settings such as color and background will customize this. The following items will appear on the Desktop by default each time a user logs on.

1. **Taskbar:** The taskbar lies along the bottom of the screen and lists the windows that are currently open. To switch from one window to another, click the desired window's name from its button on the taskbar.

2. **Start Button:** The Start button is in the bottom left corner of the screen. The user can use Start to quickly initialize a program or find a file. It is also the fastest way to get Windows help.

3. **Icons:** Icons are pictures that represent files, programs, folders, printer jobs, or computers. Icons provide a shortcut or faster way to open the item.

4. **My Computer:** The user can use the My Computer icon to quickly and easily see everything on his/her computer. Double-click the icon to browse through the files and folders.

5. **Network Neighborhood:** If the user is using a network, this icon appears on the desktop. The user can browse through the computers in his/her workgroup or network by double-clicking on the icon.

6. **Recycle Bin:** Windows stores deleted files in the Recycle Bin. The user can use the Recycle Bin to retrieve files deleted in error or empty the Recycle Bin to permanently delete the files.

7. **RAPIDS:** The user can double-click the RAPIDS icon to start the RAPIDS application.

8. **RAPIDS Bar Code Reader:** The user can double-click the RAPIDS Bar Code Reader icon to run the bar code reader application.

9. **QWS3270 Emulator:** The user can double-click the QWS3270 icon to access the AHSMC and DEERS mainframe applications by running the 3270 terminal application if the server site has been loaded with this application. Due to firewall issues, not all sites will have this icon available to them. **Appendix I** contains step-by-step directions on the use of QWS3270 for authorized sites.

10. **RAPIDS Configuration Utilities:** The user can double-click the RAPIDS Configuration icon to use the Workstation Device Configuration to view/update various RAPIDS devices. Details on using the Configuration Utilities can be found in *Section 6* of this Training Guide.

Note: In Windows Explorer the user can see both the hierarchy of folders and all the files in the folders. This is especially useful for copying and moving files. Explorer can be found by selecting **Start|Programs| Windows NT Explorer** or by right-clicking on the Start button and selecting **Explore**.

Users should always go back to the desktop to close out applications or log off the system.

4.6 Opening A Program Application

Windows NT 4.0 makes starting a program easy. The icons that are placed in the Startup folder will automatically load each time the user starts Windows NT 4.0. The user can view what is in the Startup folder by selecting **Start|Programs|Startup.** To start an application that was not started automatically, double-click on the desired icon on the desktop.

4.7 The Window

The Window is a framed region on the screen that displays information. The following are the different parts of a window.

1. The **Title Bar** is the topmost strip in any window. It lists the name of the program, as well as the name of any open file. When the user is working in a window, its title bar is highlighted, meaning that it is a different color from the title bar of any other open window.

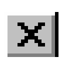
2. The **Title Text** represents the name of the object, document, or application being viewed in the window (in this case it would be RAPIDS).

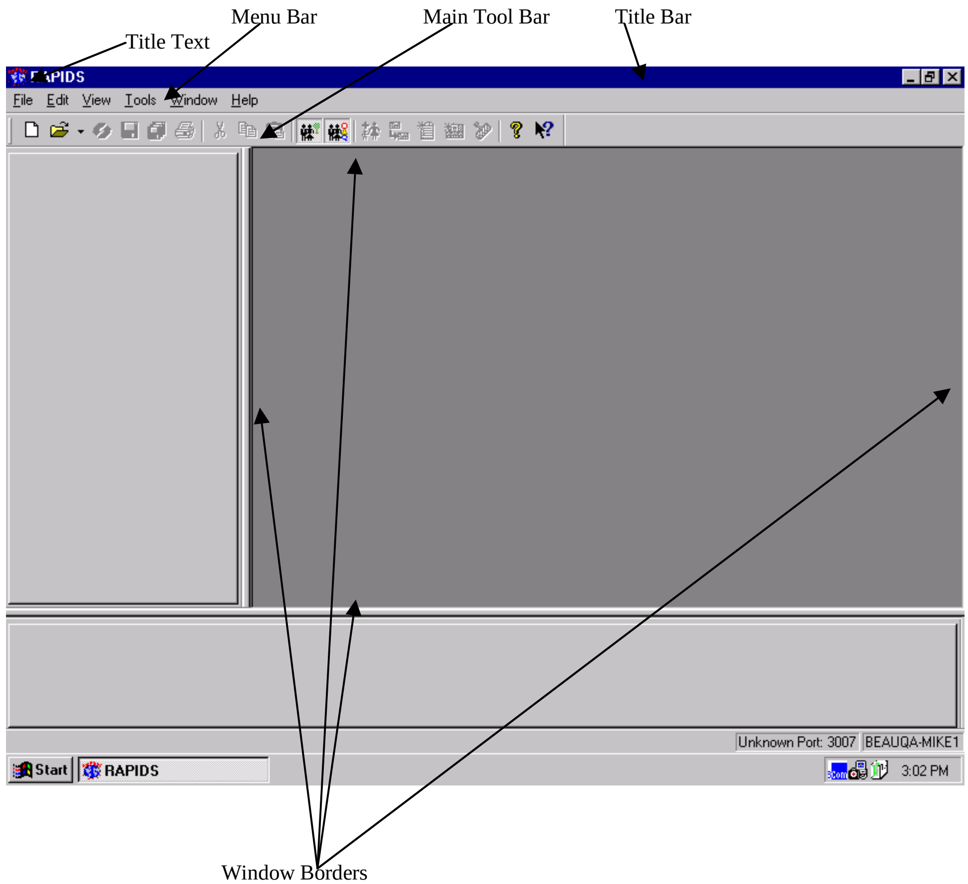
3. Windows NT 4.0 hides its menus in a **Menu Bar**. Lying beneath the title bar, the menu bar keeps those menus hidden behind key words. After selecting a key word, a list of options related to that particular key word will appear underneath. These are often referred to as pull-down menus.

4. The **Toolbar** is located just below the menu bar. It consists of buttons/icons that represent commands the user would normally access using the pull-down menus. Notice that when the mouse pointer is moved to the icon, the name of the icon appears.

5. The **Window Borders** are the four edges that define the border of the window. Borders can be adjusted by pointing on them and dragging them in or out.

6. The **Scroll Bar** is along the right or bottom edge of a window. By pointing and clicking while inside the scroll box on the right side allows the user to travel up and down while paging through his/her work. The position of the scroll bar allows the user to determine whether he/she is near the top, the middle, or the bottom of a document. Scroll bars that run along the bottom of a window can move the view from side to side rather than up and down.

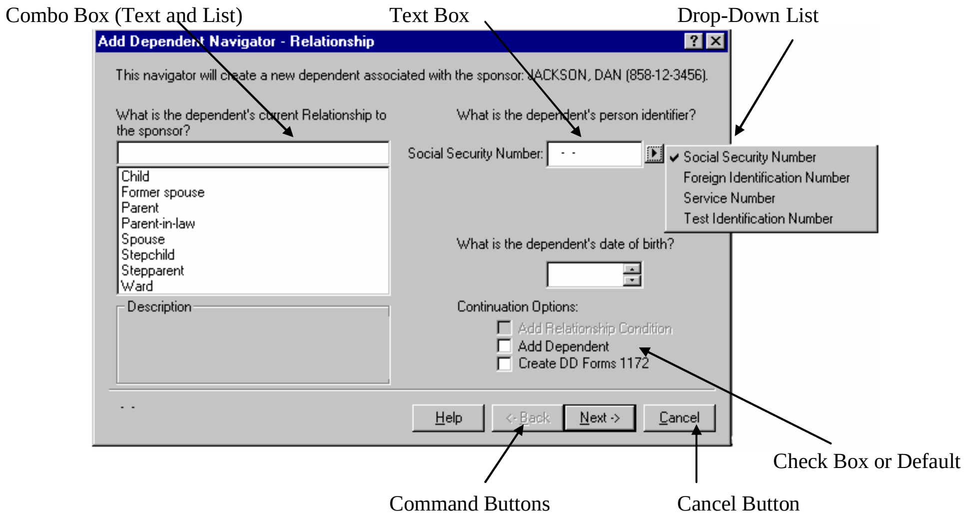
7. The **Close** button  is located in the top right hand corner of the window. Choosing this button will close the window and exit the application that is running in the window.



RAPIDS 6.x Window

4.8 The Dialog Box

A dialog box is another small window. Instead of containing a program, it contains a form or checklist for the user to fill out by maneuvering through a series of check boxes, option buttons, text boxes, or lists. Dialog boxes collect information to make decisions while running an application.



RAPIDS Dialog Box

4.8.1 Boxes, Buttons, and Lists

1. The **List Box** provides the user with a list of choices. If there are more choices than the box can display, the box contains a scroll bar to allow the user to move down the list (e.g., Branch of Service).

2. A **Text Box** is a control in which the user types text information, such as a description or a file name (e.g., sponsor's name).

3. A **Combo Box** is a hybrid control box that combines a list box and a text box. The user can select the desired item from the list box, or type the desired item in the text box (e.g., hair color).

4. **Dialog Boxes** use drop-down lists when not enough room exists for a list box. The drop-down lists have choices that can be individually turned on or off (e.g., person identifier).

5. The **Check Box Option(s)** can be individually turned on or off. When a box is blank, the option is off. When a check mark (√) or X is displayed in the box, it indicates that the option is on or selected (e.g., Joint Service Marriage [JSM]).

6. A **Default Option Button**, also referred to as an "option button," is used when the selection options are mutually exclusive (only one option is active at any one time). One option in each group of option buttons has a darkened circle. The item that is darkened is

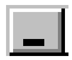
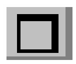
the system's default choice. If another option is selected, it is turned on and the default selection is turned off (e.g., sex/gender).

7. A **Command Button** is labeled with a specific command. Selecting a command button (e.g., **Cancel**, **OK**, **Generate**, etc.) will achieve a specified result. It initiates a command or sets an option.

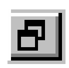
8. **Cancel** (one type of command button) halts the current operation or action and returns the system back to the state it was in before the operation or action was invoked.

4.8.2 Control

1. Sizing buttons enable the user to enlarge the window he/she wants to work in or shrink all the others so they are out of the way.

- **Clicking the** Minimize **button**  **makes its window disappear and then reappear as a button on the taskbar along the bottom of the screen.**
- **Clicking the** Maximize **button**  **makes the window enlarge, taking up as much space onscreen as possible. These buttons are found in the top right corner of the screen next to the** Close **button.**

2. When moving a window, the user must first activate the window by clicking anywhere inside the window. Next, point the mouse at the window's title bar and drag the window to its new location. When the outline of the window appears at the desired location, release the mouse button.

3. To restore a maximized window, simply click the **Restore** button  to return the window to its previous state. To restore a minimized window, click its taskbar button at the bottom of the screen.

4. To size a window, the user must choose which window border he/she would like to size, and drag that section with the mouse to create the new dimensions. (There will be a double-headed arrow for the mouse pointer on the screen).

5. When a field or dialog box contains more information than can fit in a window, vertical and horizontal **Scroll Bars** appear along the window's right and bottom edges. A **Scroll Box** moves inside the scroll bar to reflect the relative position of the current view on the screen to the entire window.

4.9 Hot Keys

The secret to using pull-down menus from the keyboard is to look for the underlined letter in each menu bar option. These underlined letters are called the hot keys. To use the menu hot keys the user must hold down ALT, press the hot key on the keyboard, and then release ALT.

RAPIDS Function	**Hot Keys**
Activate the Control	ALT+underlined letter
Add Dependent	F2
Address View	CTRL+A
Benefits View	CTRL+B
Copy	CTRL+C
Characteristics View	CTRL+H
Close Application in Use	ALT+F4
Close Current Window	CTRL+F4
Create DD Form 1172	F4
Create ID Card	F7
Cut	SHIFT+DELETE
DD Form 1172 View	CTRL+D
Display Open Programs	ALT+TAB
Family Tabs (toggle on/off)	ALT+X
Family Tree (toggle on/off)	ALT+Z
Help	F1
Help\Context	SHIFT+F1
ID Card View	CTRL+I
Insurance View	CTRL+P
New Family	CTRL+N
Next Pane	F6
Open	F9
Open from…	CTRL+O
Open Mass Issue	F11
Open Offline	F10
Paste	CTRL+V
Previous Pane	SHIFT+F6
Reopen	F5
Save	CTRL+S
Save Family	CTRL+SHIFT+S
Service Record	CTRL+R
Switch Between Views	CTRL+TAB CTRL+SHIFT+TAB CTRL+F6 CTRL+SHIFT+F6
Switch Tabs within a View	CTRL+PGUP CTRL+PGDN
Undo	ALT+BACK
Update Address	F3
Verify	F8
View Options on Start Menu (Windows NT 4.0)	CTRL+ESC
View Start Menu	Windows key

4.10 The Help Menu

If a problem is encountered with Windows NT 4.0, there are five ways to access the Help system.

1. Press **F1** for help that is context sensitive. The Help screen that appears is related to the Windows area that the user was in when he/she pressed **F1** (when an application is open).

2. Click  in a dialog box, and then click something in the dialog box. This also accesses context sensitive help; the help window that appears is related to the dialog box object that the user clicked.

3. Select **Start,** and then select the **Help** command to receive help on Windows itself.

4. In most Windows applications, the user can click **Help** in the menu bar. The Help menu that appears will have one or more commands for accessing different parts of the program's Help system.

5. **Help** appears in many secondary windows.

To access the Windows NT 4.0 Help Topics, use the following guidelines.

1. Turn on the computer to boot Windows NT 4.0.

2. At the Windows NT 4.0 desktop, select **Start**.

3. Select the **Help** menu and **Help Topics** from the list.

4. Windows Help appears.

4.11 Changing the Display to a Larger Font

If you are having trouble reading text on the RAPIDS screen, follow the instructions below to set the display to a larger font size.

1. Click **Start** from the taskbar.

2. Select **Settings|Control Panel** and double-click **Display**.

3. Select the ***Appearance*** tab from the Display Properties dialog box.

4. Under Scheme, select **Windows Standard (Extra Large)** or another larger font scheme.

5. Click **OK**. Updates apply to all applications.

6. Select **FILE|CLOSE** to close the Control Panel.

4.12 Locking the Workstation

When leaving your workstation, it is not necessary to exit completely out of the RAPIDS application unless a different VO will be using the system. Simply press the CTRL+ALT+DEL combination and click **Lock Workstation** or remove the VO's CAC. RAPIDS security will automatically lock a workstation that has been idle for five minutes. The VO must re-enter his/her unique password or CAC PIN to access the application again. If another VO needs access to your workstation, it will be necessary to exit the application and complete the following steps.

1. Exit Windows NT by clicking **Start** from the taskbar.
2. Select **Shut Down** from the list.
3. Select the option to **Close all programs and login as a different user**.
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.

4.13 Quitting Windows NT 4.0

Quitting Windows NT 4.0 is a simple task. Never turn off the computer while RAPIDS or Windows NT 4.0 is still running. Shutting down causes the temporary information stored in memory to be cleared to the hard drive. After quitting RAPIDS by selecting **File|Exit** from the main menu, and disconnecting communications to the server, the user may then shut down Windows NT 4.0. The user can shut down the operating system by clicking **Start** from the taskbar and selecting the **Shut Down** command. A dialog box entitled Shut Down Windows appears. To completely shut down the system, select **Shut down the computer?** and click **Yes**. To logoff so that another user can log in, select the option **Close All Programs and Login As A Different User**. If the user chooses the **Shut Down** option, the computer will display a screen that announces when it is safe to shut off the computer. All that is left to do is turn off the computer, monitor, and peripherals via the surge suppressor switch.

5 Becoming Familiar with RAPIDS

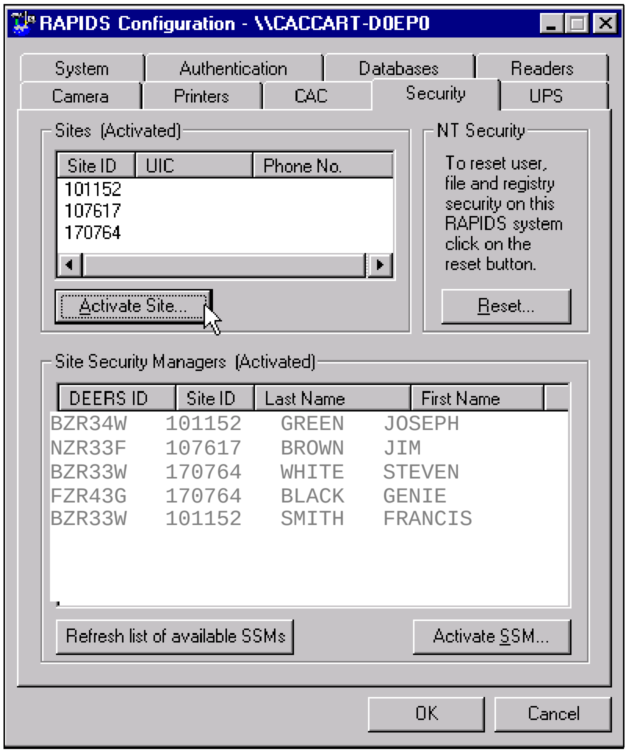
5.1 Introduction

RAPIDS is a Windows application using icons, windows, menus, check boxes, and tabs. The RAPIDS application was designed so that the user has many choices on how to complete a single task. This section contains information needed to become familiar with the new RAPIDS workstation. We will review the menu, toolbar, help functions, and main screen view.

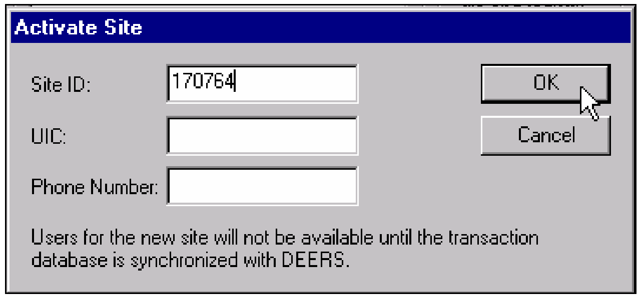
5.2 Activation of the Site and Site Security Managers

When an Installer or FSR issues the initial SSM CAC at the time of the initial RAPIDS CAC upgrade, the following procedure is required. This segment details the required addition and activation of sites and SSM's to the CAC RAPIDS 6.0 server.

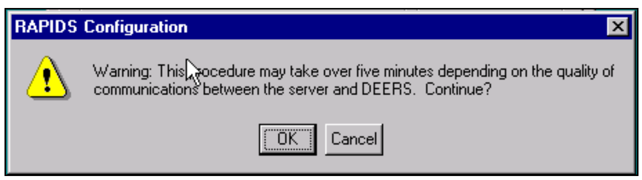
1. Log in to the Server as Administrator and Open RAPIDS Configuration to the ***Security*** tab.



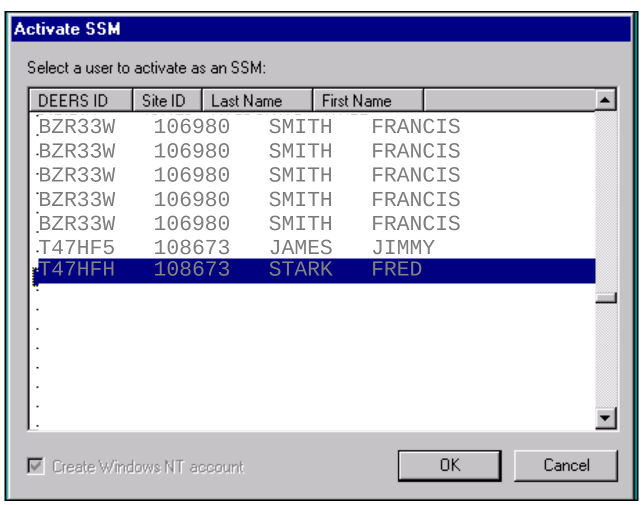
2. Click on the Activate Site button and enter site number 170764 for the Field Service Representative. Repeat this step for site 107617 for the Installers' site in addition to the current RAPIDS sites as required. This will add the site IDs to the Activated Site list.



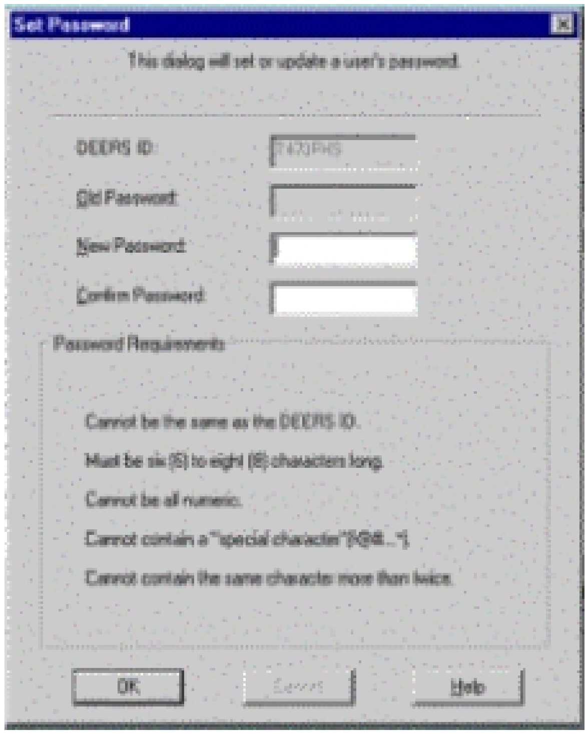
3. Refresh the SSM list to add the SSMs from the newly added sites to the Site Security Managers (Activated) pick list. The refresh can be performed at the server or the workstation.



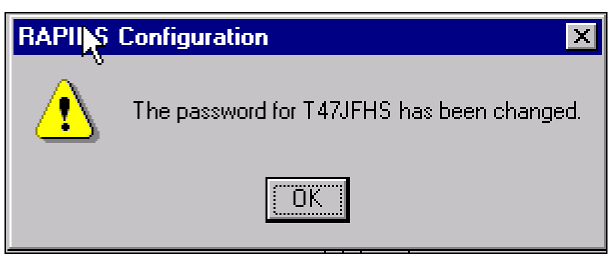
4. Once refreshed, select each SSM to activate. Follow the instructions in the Set Password dialog box. These password requirements apply to all NT passwords under the new security system. Note that NT will prompt the user to change this password upon the first SSM login attempt.



5. Follow the instructions in the Set Password dialog box. If the strong password filter is enabled, Windows NT will require a complex password (including upper, lower, special characters and a number). NT will prompt the user to change this Password upon the first login attempt. Once complete, you are ready to log into a workstation and produce the SSM's CAC.



Note: In RAPIDS 6.0, all NT passwords (whether complex or simple) are set to expire every 90 days.



5.3 Logging in to RAPIDS 6.0

Login activities are controlled by the ActivCard Gold middleware application. When the VO powers on a RAPIDS 6.0 workstation or server, the usual NT login screen is replaced by the ActivCard Gold login. The initial login requires the VO to set his/her NT Login account to allow login with the CAC. To do this, the VO must log in without the CAC inserted and use his/her DEERS ID and the NT password. In most cases for users being upgraded from RAPIDS 5.2 to

6.0, the initial RAPIDS 6.0 NT password will remain the same as the RAPIDS 5.2 password. Once the VO has updated his/her CAC with the NT Login ID and password (as detailed in the following sections), the VO can (and should) use the CAC and PIN to log in to a RAPIDS 6.0 workstation. **No cards should be left in the VO or card recipient encoder/reader when the VO is away from the RAPIDS workstation.**

Note: Establishing the connection with the RAPIDS server is dependent upon each site's communications infrastructure, which varies among sites.

Hybrid RAPIDS sites (those with RAPIDS 5.2 and RAPIDS 6.0 workstations running simultaneously) should routinely login to the RAPIDS 5.2 workstation using their DEERS ID and password. Users should routinely log in to RAPIDS 6.0 workstations using the CAC and PIN.

Each RAPIDS user prior to logging in to the RAPIDS workstation with their VO CAC must accomplish two tasks: (1) set the NT Login Account and (2) register the user's certificate on the workstation. These steps are required for each individual user and should also be repeated for each SSM/VO CAC issued, taking care to have each new VO logged in using their own DEERS log in ID to register their own certificates. An additional step of Adding Dial-up Settings is necessary for VOs at workstations that are dialing into a RAPIDS server.

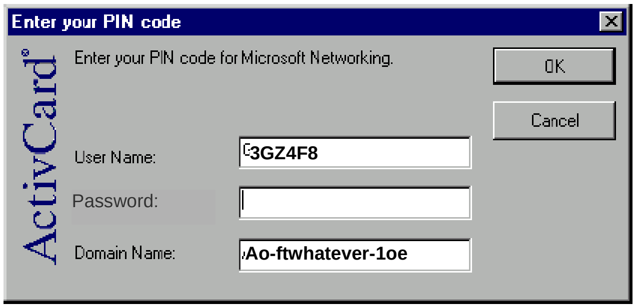
Note: If logging in with a DEERS user ID, the RAPIDS application will start automatically, unless you are assigned NT Administrator privileges. Select the "Cancel" button on the RAPIDS progress meter before proceeding with the following steps. All users will need to complete these steps before they are fully functional as RAPIDS 6.0 VOs.

There are two methods for logging into the RAPIDS 6.0 workstation:

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

5.3.1 First Time Login with Login ID and Password

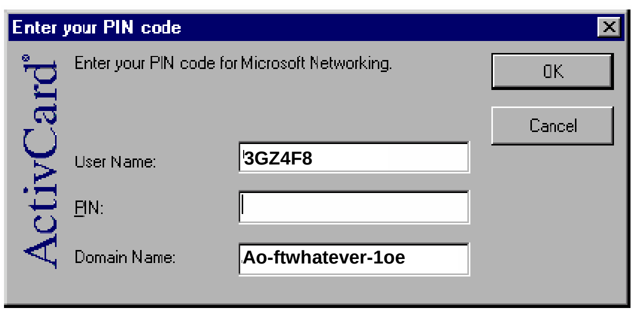
First time users of a RAPIDS 6.0 workstation must remove their CAC from the VO encoder/reader and input their DEERS user ID and use their DEERS password in place of their PIN as the two have not yet been associated through ActivCard Gold.



The VO must set an NT login account through the ActivCard Gold application at any of the site's workstations. This task is detailed in *Section 5.3.3* of this Training Guide.

5.3.2 Logging in with a CAC and PIN

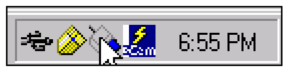
Once the Windows NT Login has been added, insert the VO's CAC into the VO encoder/reader. Within a few seconds, the VO's DEERS ID will populate the User Name field and the VO will be prompted for a PIN instead of a Password. When typing a PIN, ensure that the Number Lock key is selected.



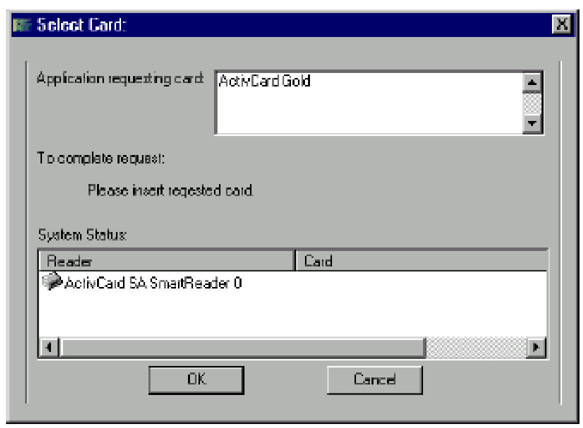
5.3.3 Setting the NT Login

Access to the RAPIDS 6.0 domain at each site is mediated by the ActivCard Gold middleware. The VOs must set an NT login account through the ActivCard Gold application at any of the site's workstations.

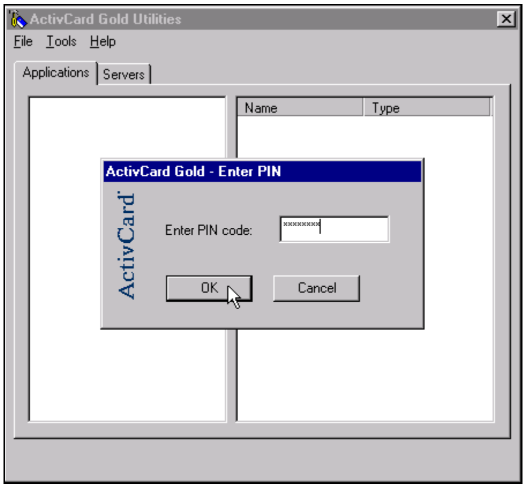
1. Insert the card that needs registration into the VO encoder/ reader. This would be the CAC for the VO logged on to RAPIDS.
2. Double click on the ActivCard Gold Icon in the System Tray.



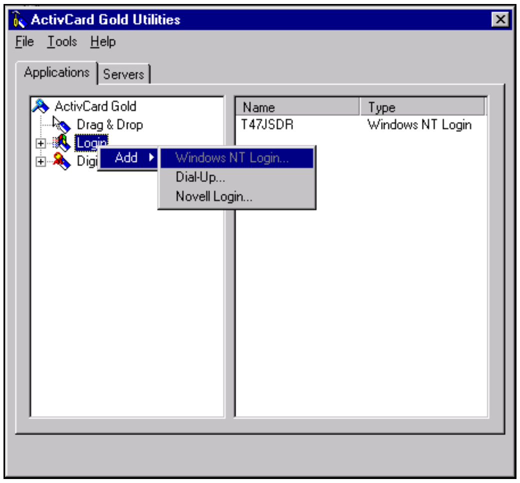
3. On occasion you may be asked to select which card reader your CAC is in. As a rule, when logging in, be sure that there is not a CAC in the card recipient encoder/reader.



4. To set the NT Login account so that VO can login to NT using his/her CAC, ensure that the VO's card is inserted into the VO encoder/reader.

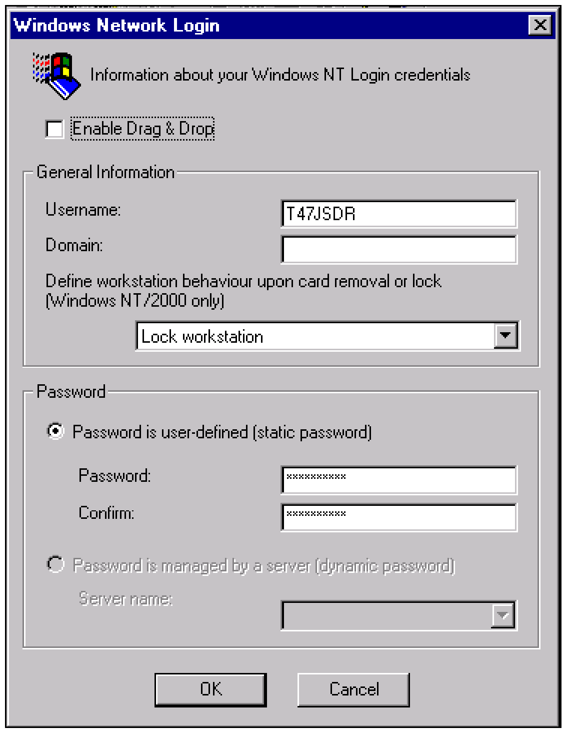


5. Right-click on the Login option in the left window of the ActivCard Application and select Add|Windows NT Login from the menus. This process needs only to be completed at one workstation connected to the RAPIDS server.

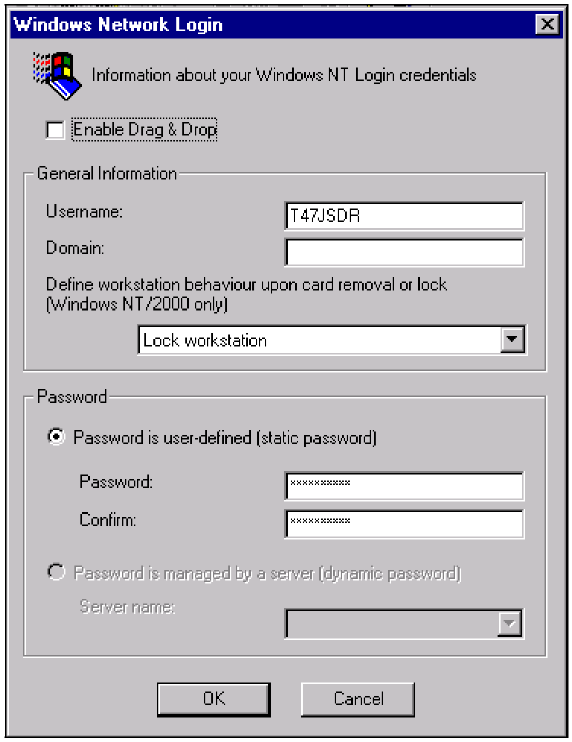


6. At the Windows NT Login dialog box, type in the User Name (DEERS login ID) in UPPERCASE. Site users should input their RAPIDS domain name. This can be found by pressing CTRL+ALT+DELETE and reading it from the ActivCard Graphical Identification and Authentication (GINA) screen. Verify that the option to “Define workstation behavior upon card removal or lock” is set to “Lock Workstation.” No other option is acceptable.

Note: Installers and FSRs should leave the Domain Name blank.



7. Have the VO enter and confirm their NT password (this may match the DEERS password in users who were previously using RAPIDS 5.2), and press **ENTER**. This VO may now use his/her CAC to log in to that RAPIDS 6.0 workstation and perform VO functions. The VO must now follow the procedures detailed in the *Section 5.3.4* at each RAPIDS 6.0 workstation at their facility.

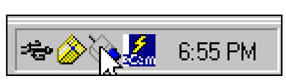


Note: If Windows NT is not set up with a strong password filter, the VO should enter the password in ALL CAPS.

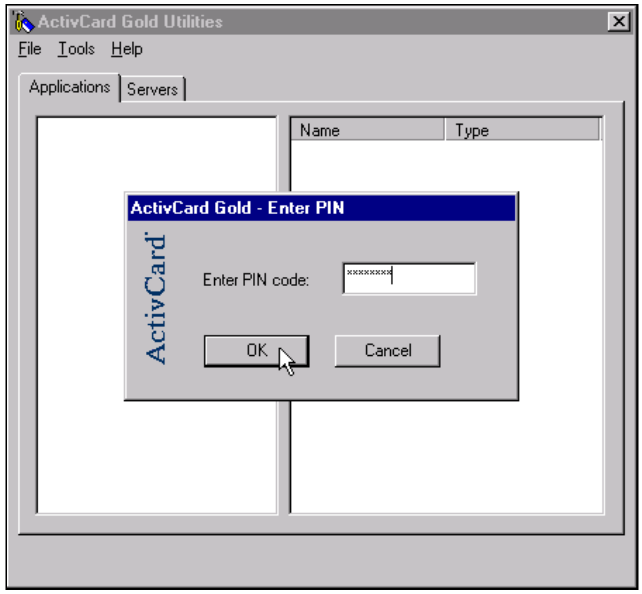
5.3.4 Registering Certificates

Prior to logging into RAPIDS, user must register their identity certificate to the RAPIDS workstation using the following procedure. This procedure must be performed at each RAPIDS workstation to which the VO wishes to login.

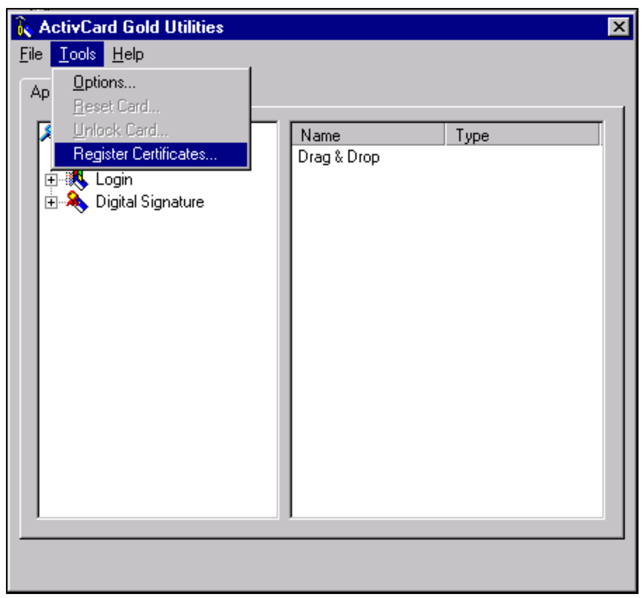
1. Insert the card that needs registration into the VO encoder/reader. This would be the CAC for the VO logged in to RAPIDS. Double click on the ActivCard Gold Icon in the System Tray.



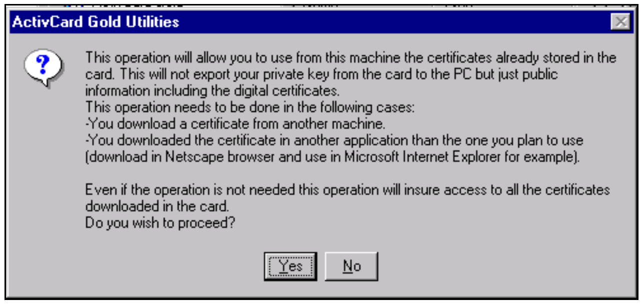
2. When prompted, enter the PIN for your CAC.



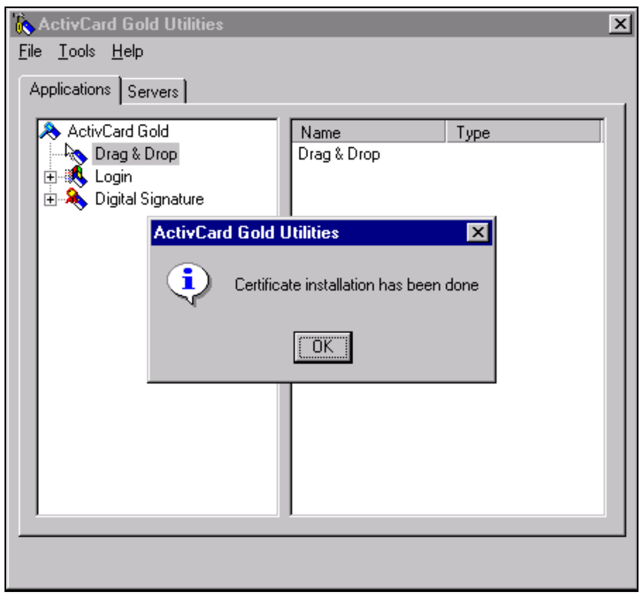
3. The RAPIDS user registers his/her certificate by selecting Register Certificates from the Tools menu.



4. 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 has been done," should appear. This registration process must be completed at each RAPIDS workstation for which the VO needs access.



5.3.5 Adding Dial-Up Settings

Users at workstations that are dialing into a RAPIDS server must complete the additional step of entering information about their workstation's specific dial-up settings.

1. Ensure that the VO's card is inserted into the VO encoder/reader. After registering the certificate through the ActivCard Gold application, right-click on the Login option in the left window of the ActivCard application and select **Add|Dial Up** from the menus.

2. At the Dial-Up Settings dialog box, enter the User Name (DEERS login ID). Have the VO enter and confirm his/her NT password (this may match the DEERS password in users who were previously using RAPIDS 5.2) and press **ENTER**.

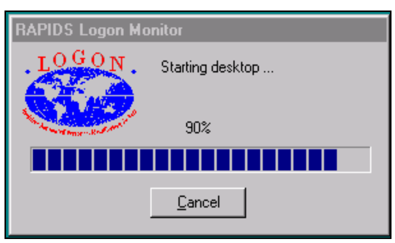
Note: If Windows NT is not set up with a strong password filter, the VO should enter the password in ALL CAPS. This VO may now use his/her CAC to log into that RAPIDS 6.0 workstation and perform VO functions.

3. In the Connection Parameters section, select the proper entry name from the drop-down list. It may be necessary to copy the parameters from the SSM's dial-up settings window or work with the communications POC to select the correct parameters for your site.

5.4 Starting RAPIDS

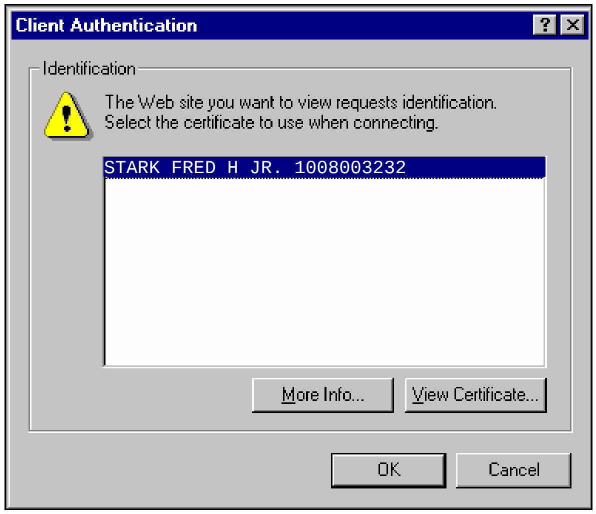
After the RAPIDS user has (1) Registered the user's certificate, and (2) Set the NT Login Account he/she can start the RAPIDS application. A check to verify the VO's identity certificate will be performed before allowing DEERS activity. DEERS will check and store the CA's CRLs to ensure that the VO's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

Insert the VO's CAC into the VO encoder/reader. Press CTRL+ALT+DELETE to display the login screen. When prompted, enter the six to eight digit PIN. 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 NT desktop appears before proceeding to step two. The application will display a progress meter as the Windows NT desktop opens.

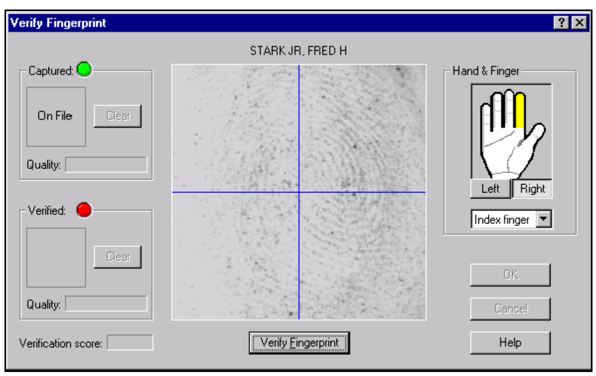


The RAPIDS application should start automatically. If the RAPIDS progress meter does not appear, double-click the RAPIDS icon. The application will display the RAPIDS logo while the computer starts the application. The VO will be prompted to select his/her certificate during the start-up process. Select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

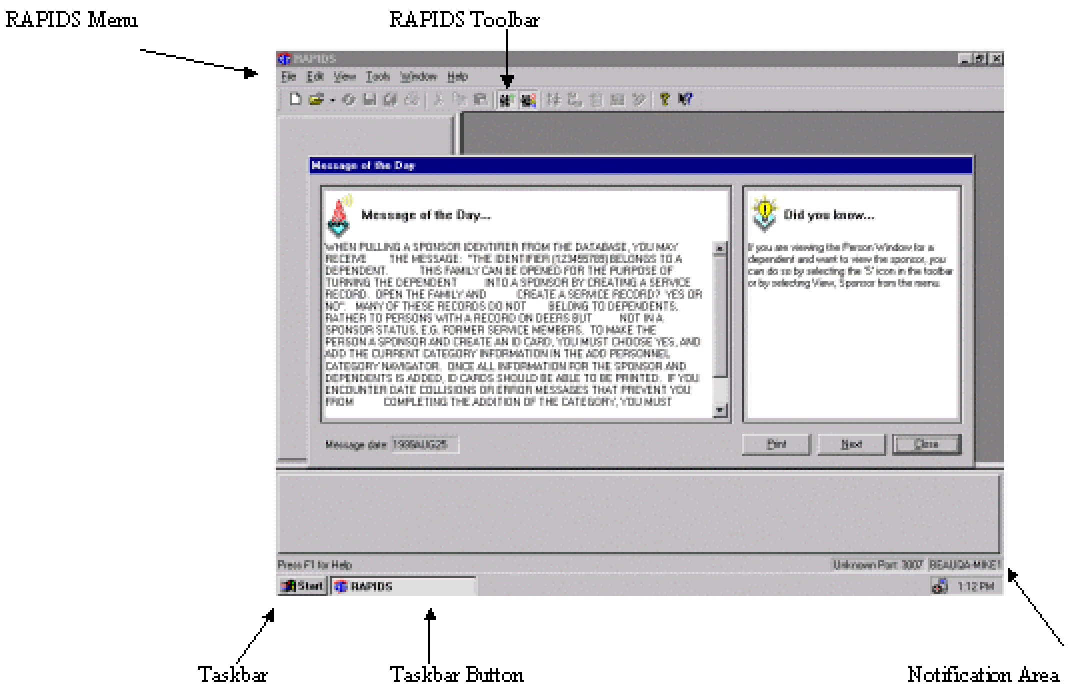
If the certificates are not registered, RAPIDS will display a blank Client Authentication dialog box.



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

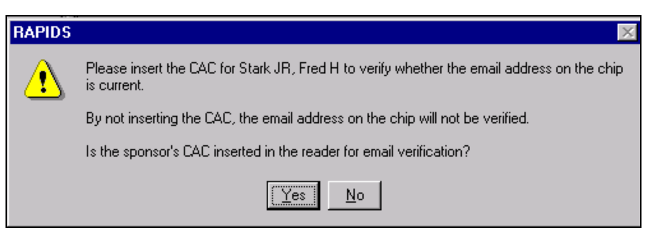


When the application is up and running, the “RAPIDS Message of the Day” is displayed. When viewing the message for the first time, the “Message of the Day” will be highlighted in red. Print the Message of the Day by clicking **Print** in the dialog box. Click **Next** to allow the VO to scroll through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



Initial RAPIDS Screen

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.



Note: 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. Refer to *Section 4* of this Training Guide for guidance on unlocking a workstation that has been locked.

RAPIDS SSMs should log in to Windows NT 4.0 and RAPIDS as described above for all users. Refer to *Section 9* for the steps necessary for SSMs to activate and select roles for other RAPIDS users.

5.5 Opening a Family in RAPIDS

To open a family record in RAPIDS, the VO must input his/her CAC into the 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.

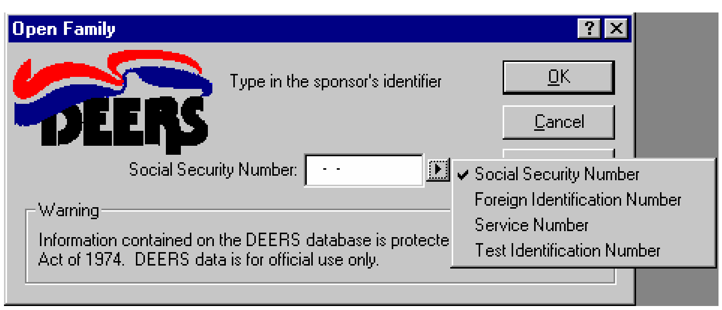
   Note: The downward pointing arrow allows the user to select the location from which the family is opened.

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.

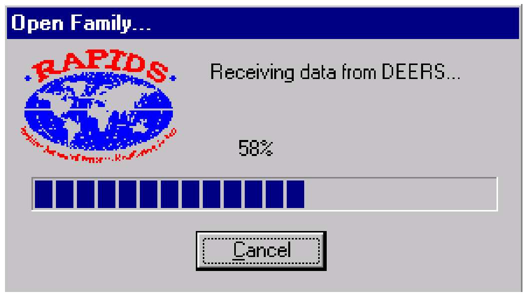
   Note: If the sponsor does not have a valid SSN, click the right pointing arrow next to the SSN field. A box will appear allowing the user to select from other Sponsor Identifiers, such as Service Number or FIN.



Open Family Dialog Box

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.



Open Family Progress Bar

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.

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.

5.6 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.

5.7 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.

5.8 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 **Tool**s 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 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 SPOs only). Every command under Family will give the option to update multiple family members.

5.9 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 SPOs 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.

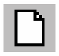
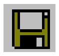
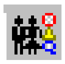
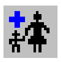
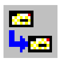
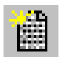
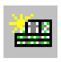
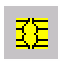
6. **Verify:** Allows you to record the verification of a person's dependent status.

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.

5.10 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.

5.11 RAPIDS Help (Using Online Help)

While working in RAPIDS, Online Help is available for both Windows NT 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.

5.11.1 RAPIDS Help from the Menu

RAPIDS Online Help within the RAPIDS application is found in the drop-down list under **Help** on the main 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 the same 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:\Program Files\DMDC\RAPIDS\Data\Document**.
4. Open the desired section and select **File|Print** from the menu.

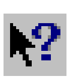
Other selections on the menu include **Message of the Day**, which allows the VO to view the message and tip of the day, and **Privacy Act**, which displays the Privacy Act Statement and the conditions applicable to sponsor or applicant.

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.

5.11.2 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 to close it.

5.11.3 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.

5.11.4 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 Referring to RAPIDS Online Help

The RAPIDS Online Manual and Online Help are divided into the following major sections.

1. **Introduction:** A discussion of the organization of the manual and Online Help, the system, history, and missions of activities, organizations, systems associated with the RAPIDS application, the redesign concept, and the RAPIDS User Manual and Online Help design and breakdown.
2. **Getting Started/RAPIDS Tutorial:** A detailed discussion of workstation and server functionality and how to perform tasks particular to each.
3. **The RAPIDS User Interface:** A detailed discussion of commands used by the RAPIDS application.
4. **Common Data Processing Scenarios:** RAPIDS processing information guide and instructions for creating ID cards, DD Forms 1172, and related functions.
5. **Security and User Accounts:** A detailed discussion of system and user security, users' definitions, privileges and responsibilities.
6. **Reports:** Report processing information guide and instructions for completing various reports (e.g., audit trails).
7. **Site Administration:** A detailed discussion of offline processing and site and user administration.
8. **Deployable RAPIDS:** A detailed description of RAPIDS systems configured as deployable.

9. **High Volume RAPIDS:** A detailed description of RAPIDS systems configured as high volume.

10. **Resources and Contacts:** A list of POCs who can assist with various DEERS/RAPIDS problems, concerns, and issues.

11. **ID Card Information:** The sponsor's status and the abbreviations that appear on sponsor's and dependent's ID cards, relationship to the sponsor that appears on ID cards, and the blocks of information found on the ID card.

12. **Military Ranks and Grades:** Tables that include the military ranks and grades for each Service, branch of Service with the Service seal, and abbreviations that appear on sponsor's and dependent's ID cards.

13. **Error and Warning Messages:** An explanation of communications problems and a list of system errors.

14. **Frequently Asked Questions about RAPIDS:** A list of questions and answers about RAPIDS.

15. **DEERS Database Access:** A discussion of how to access the DEERS database through your RAPIDS workstation.

16. **Using RAPIDS without a Mouse:** A discussion of the keys and key combinations that perform the same functions as the mouse.

17. **Privacy Act Statement:** In accordance with the Privacy Act of 1974, RAPIDS users are not free to disclose the information contained in a person's DEERS record. Additionally, DEERS data cannot be used for any reason other than those listed by the Privacy Act Statement.

    However, a beneficiary's eligibility start and end dates may be released to persons with a valid need to know.

18. **Glossary of Terms:** A list of commonly used acronyms, terms, and definitions.

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, 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, 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.

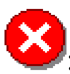
5.14 Family Tabs

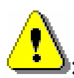
The ***Family*** tabs are located on the bottom of the RAPIDS screen. These tabs include ***Tasks***, ***Tree Details***, and ***Sponsor Confirmation*** information.

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.

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.**
- 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, which are the same as the 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 S (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 Functions and Features of the RAPIDS Application

6.1 Introduction

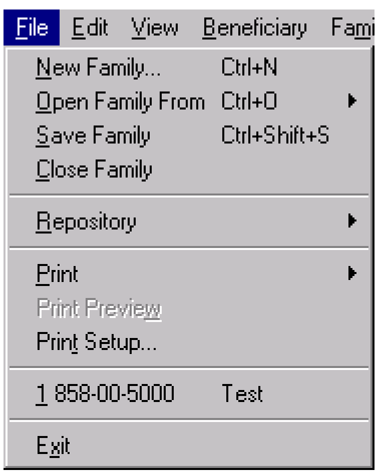
This section explains the major functions of RAPIDS and the navigators and viewers used to apply these functions. The user will learn how to differentiate between a category and a condition and be introduced to special features used to customize each workstation.

6.2 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 many 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.

6.2.1 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**, **Off-line Repository**, **PDF417 Bar Code**, and **Mass Issue Repository.**



6.2.2 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 6.1.2* 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

6.2.3 What is the Difference between a Personnel Category and a Personnel Condition?

It is very 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.

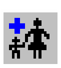
A family member dependent will have a Relationship Category and may have one or more Relationship Conditions (see *Section 6.2.4*). Only certain conditions are available for certain categories. When a category/relationship is terminated, it displays a red **X** in the family tree. This alerts the user that this category/relationship has been terminated.

6.2.3.1 Personnel Categories and Their Related Conditions

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

Category	Applicable Conditions
Non-Government Agency Personnel	Non-CONUS Assignment Living in Quarters
Other Government Agency Contractors	Non-CONUS Assignment Living in Quarters Emergency Essential-overseas only Emergency Essential-CONUS Emergency Essential-CONUS/living in quarters
Other Government Agency Employees	Non-CONUS Assignment Living in Quarters Emergency Essential-overseas only Emergency Essential-CONUS Emergency Essential-CONUS/living in quarters
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

6.2.4 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.

Open Dependent Dialog Box

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).

5. 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.

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

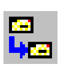
   The following table lists valid RAPIDS Relationships and their applicable relationship conditions. By adding a relationship condition, the dependent’s benefits or eligibility dates could change to reflect appropriate benefits.

Relationship	Relationship Conditions
Child	Lives with entitled Former Spouse Sponsor provides 50% Support Less than 50% Support Accompanying Sponsor Terminate entitlement under Sponsor
Former spouse	[None]
Parent	Accompanying Sponsor

Relationship	Relationship Conditions
Parent-in-law	[None]
Spouse	Accompanying Sponsor Terminate entitlement under Sponsor
Stepchild	Lives with entitled Former Spouse Sponsor provides 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 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.

6.2.5 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 cards.

1. From the main 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.

6.2.6 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 main 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 50% Support” should be added to children not residing with the sponsor and not entitled to commissary benefits. In addition, no condition or suspension of benefits should routinely be added to those children under the age of ten.

6.2.7 Verify Dependents

The  Verify Dependents tool was created for sponsors to update their dependents’ eligibility information. The sponsor signs the DD Form 1172 and 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.

It is important to note the following.

1. 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.

2. 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 was issued.

Note: 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.

6.2.8 DEERS/RAPIDS Fingerprint Capture Process

The Fingerprint Capture dialog allows the user to capture a fingerprint for all sponsors processed by RAPIDS. A fingerprint will be 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, 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.

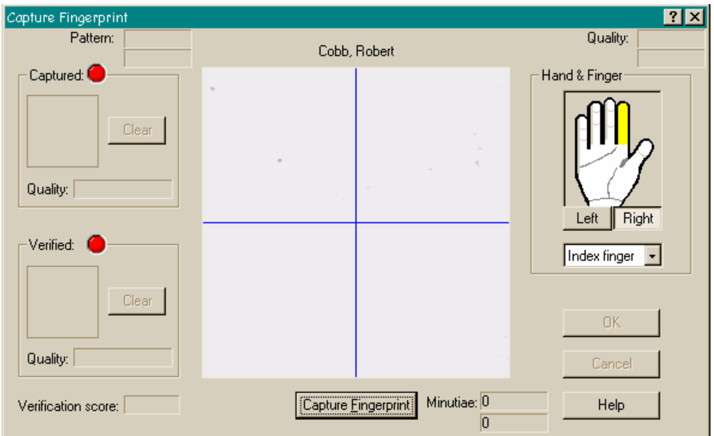
In RAPIDS 6.0, when producing a CAC, RAPIDS will ask the VO to match the sponsor's fingerprint with the fingerprint stored on the DEERS database. Considerable enhancements have been made to the quality of the fingerprint captured. These enhancements increase the chances of a positive match when a biometrics 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 can be captured by 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.

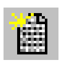


6. The default fingerprint captured should be the right index finger. This can be altered if necessary by selecting the hand and finger used from the upper right hand side of the Capture Fingerprint dialog box. Position the individual's right index finger on the fingerprint scanner. Notice that the fingerprint 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 **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. If the individual is younger than 40 years, the fingerprint must be captured every nine years. If he/she is 40 years or older, the fingerprint is captured every three years.

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.

Note: The 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.

6.2.9 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.

4. 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 6.13.9*).

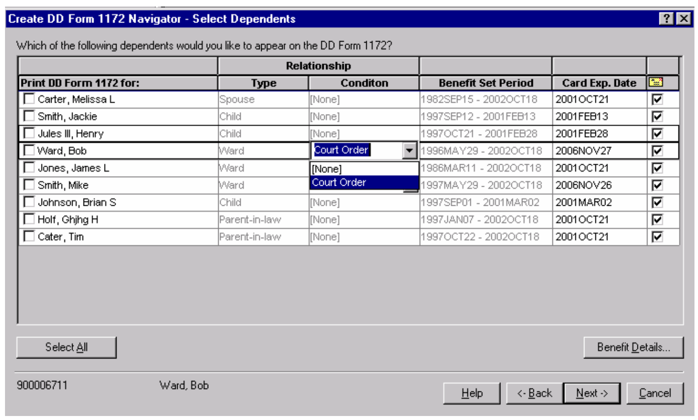
When the Default Remarks check box is deselected, the user will be prompted to select the remarks that need to appear on the DD Form 1172. The VO can select from the available list of RAPIDS remarks by double-clicking on a specific remark. The VO may also enter his/her own remark by typing it in.

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 segments 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.



RAPIDS Select Relationship Condition Window

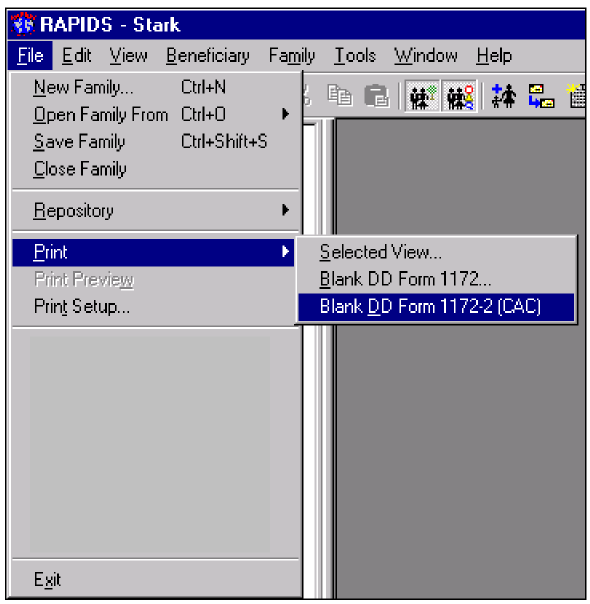
Note: To ensure that the DoD has an archive of historical DD Forms 1172 on file, the DSO will accept paper DD Forms 1172 from ID card facilities for archiving electronically. Only DD Forms 1172 for family members need to be forwarded. Supporting documentation (such as marriage/birth certificate) should 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. These forms should be sent to:

DMDC Support Office
Attn: 1172 Scan
400 Gigling Road
Seaside, California 93955-6771

6.2.10 Create DD Form 1172-2

The 1172-2 is the application for DoD CAC and DEERS enrollment. This form is to be provided to the VO for entry of DoD Civilians and DoD Contractors into DEERS. The form should also be used when adding a Personnel Category of DoD Civilian or DoD Contractor to an existing sponsor's record. A blank DD Form 1172-2 can be printed through the RAPIDS 6.0 application by selecting **File|Print|1172-2** from the menu. Until a policy is distributed, sites should maintain the copy of the DD Form 1172-2 presented to them by DoD Contractors and DoD Civilians.

The 1172-2 is an additional form used to enter a DoD Civilian employee or Contractor into DEERS. This form is to be given to a DoD Civilian employee or Contractor to be completed, signed, and returned for entry into DEERS. To print this form, select the Blank DD Form 1172-2 (CAC) option from the Print submenu of the File menu.



6.3 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. The JDM smart card supported in previous versions of RAPIDS is not detailed in this RAPIDS Training Guide and is not supported in the current version of RAPIDS software.

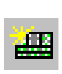
6.4 Using RAPIDS 6.0 to Issue the CAC

With a few minor exceptions, the RAPIDS CAC software looks virtually identical to the previous versions of RAPIDS software, with the added capability to produce the CAC. The VO's Windows NT login ID and password are stored on his/her CAC. Special software has been added to Windows NT that uses the login ID and password from the VO's CAC to log in to the RAPIDS workstation when the VO's PIN is entered. When the VO's CAC is removed from the encoder/reader, 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.**

The CAC software and hardware differs from the previous RAPIDS 5.x ID card system in the following ways.

1. RAPIDS 6.0 uses a PVC card printer designed for printing the plastic CAC. This printer does not have the capability to print on plain paper.
2. Two separate smart card o r r r are used. One is used to read the VO's card to log in and establish the SSL session. The second writes and reads data to the CAC recipient's computer chip.
3. A numeric PIN pad allows the CAC recipient to enter his/her PIN number. When the CAC is issued, the card recipient chooses a six to eight digit PIN and enters it using the PIN pad. The PIN is encoded into the ICC.
4. The work e-mail address has been added to the RAPIDS Service Record View. This information is used in the certificate for encrypting e-mail. Multiple cards mean multiple certificates will be generated. An Agency/Sub-agency field has been added for DoD Civil Service and DoD Contractors.
5. The EDIPI is now included in all media on the CAC. This identifier is used to uniquely identify individuals to make sure DoD refers to the same person throughout various systems (RAPIDS, CHAMPUS, etc.). It is not displayed anywhere on the card.
6. A biometrics (in the form of a fingerprint) is used to verify the VO and the CAC recipient/cardholder during PIN changes or unlocking the CAC.
7. RAPIDS allows the termination date for the CAC to be entered. This allows for certificates to be revoked on the date specified.
8. A new data field, Organ Donor, is now displayed on the CAC and within the RAPIDS software. This information can only be updated through the military medical facility.
9. A new form, the Application for Common Access Card, DEERS Enrollment (DD Form 1172-2) can be printed through RAPIDS.
10. A new data field, Country Assigned, is captured within the RAPIDS software.
11. A record of certificate issuance is stored on DEERS to give DEERS/RAPIDS reporting and revocation capabilities.

6.4.1 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 6.2.8).

4. At the Modify Photo screen, adjust the camera using the onscreen buttons. 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.

6.4.2 CAC Issuance Process Flow

When creating a CAC, follow the procedures as listed in the AFI 36-3026 and the VO Certification Practice Statement (CPS) to verify all information currently verified 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 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 <u>before</u> creating the CAC. This information can only be updated through the medical application at their military medical facility. If they wish to change their organ donor status, direct them to their nearest military medical facility before creating a CAC.

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 1172-2 to enter them into DEERS through the Add Personnel Category navigator. Please refer to the Required Fields table below, as not all information from the Characteristics screen (such as height and weight) is required to add a DoD Civil Service, DoD Contractor, or Foreign National. The following is a table of required fields for these personnel categories.

DoD Civil Service	**DoD Contractor**	**Foreign National Employee**
Personnel Category	Personnel Category	Personnel Category
Name	Name	Name
Date of Birth	Date of Birth	Marital Status
Gender	Gender	Date of Birth
Pay Plan/Pay Grade	Pay Plan/Pay Grade	Gender
Date of Employment	Date of Employment	Pay Plan/Pay Grade
End of Contract	End of Contract	Date of Employment
Service/Organization	Service/Organization	End of Employment
	Contract Type	Country of Origin

Enter a blood type (or UNK) for DoD Civil Service, DoD Contractor, or Foreign Nationals.

For the End of Contract / Employment field, the VO should enter the end date of three years from the Issuance date or the Contract End Date. Family members should 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).

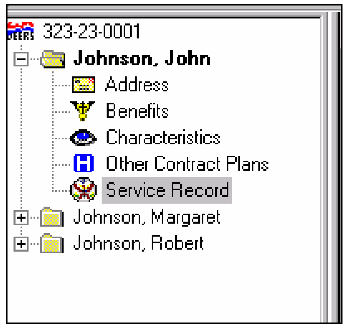
Note: Civilian personnel tapes send the birth month and year for Civilian employees to DEERS. Since the actual birthday is not sent to DEERS, the first of the month may display. VOs should confirm (and update if necessary) the date of birth on all DoD Civilians.

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.

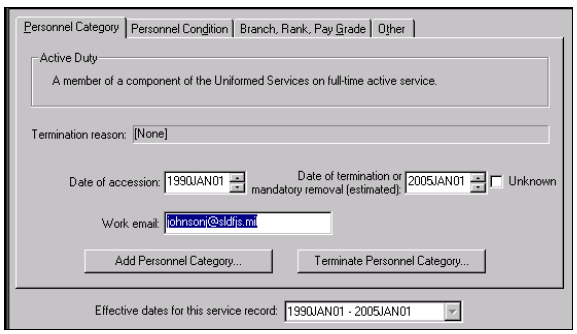
To create a CAC, use the following procedure:

1. Open Family from DEERS.

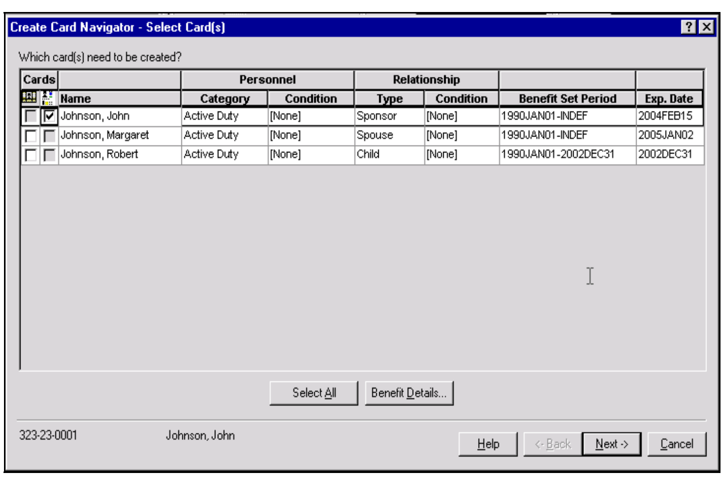
2. If the Family is new, create a new family from the signed DD Form 1172-2.



3. Verify/enter all sponsor information as detailed in the table above. **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.

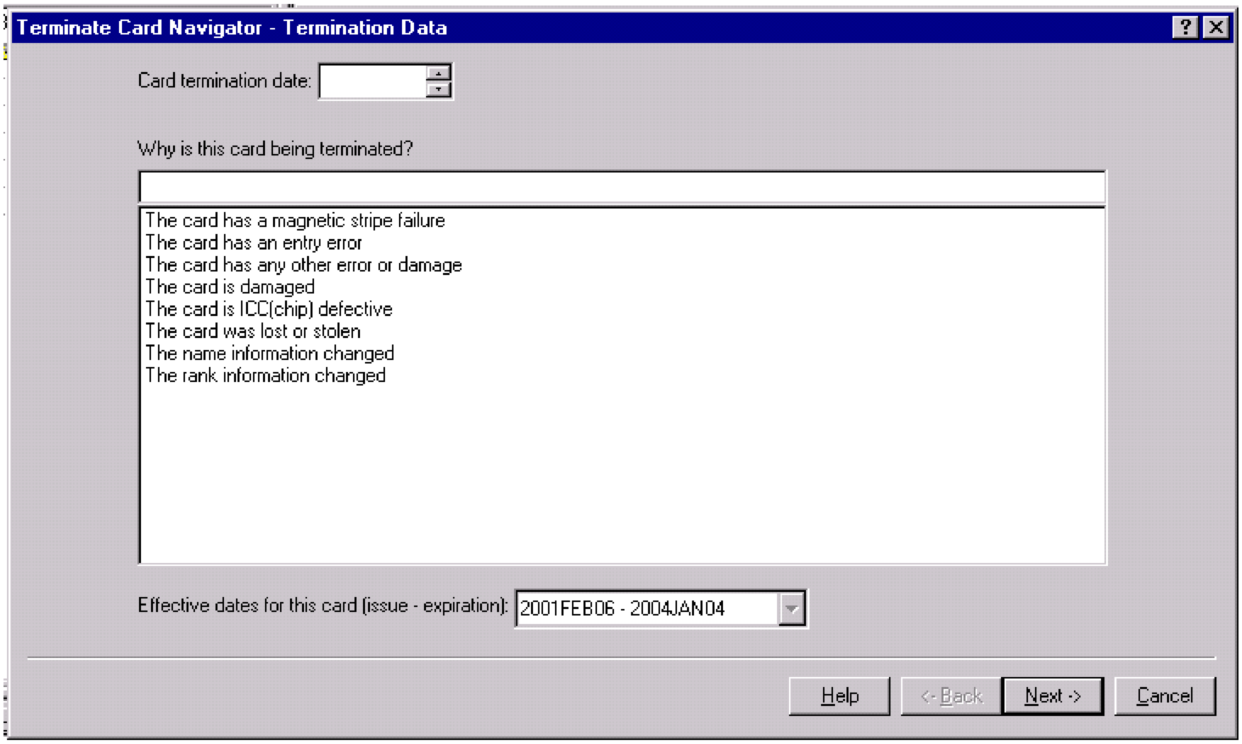


4. When opening the Create Card Navigator, the Cards field at the left of the Navigator dialog box contains two icons. Click on the **Create Card Icon** and check the Sponsor's CAC checkbox to the left of the sponsor's name.



Note: Family members and retirees are not currently 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.

5. Enter a card termination date and select a reason for terminating the previous card from the list.

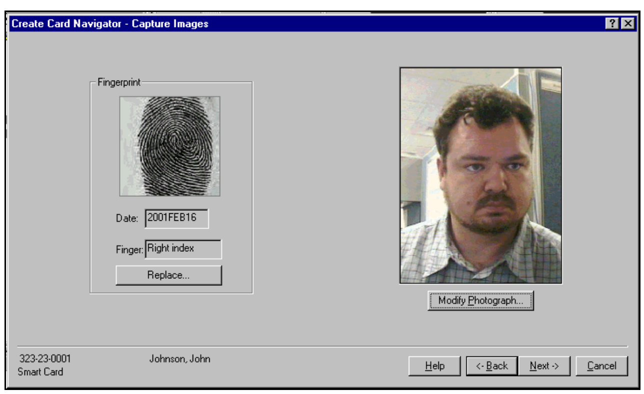


6. Capture Fingerprint. When issuing a CAC, RAPIDS will prompt the VO to capture the sponsor's fingerprint. If the sponsor's DEERS record has a prior fingerprint stored, RAPIDS first verifies that the fingerprint matches the previous one in DEERS. This allows the VO to verify the CAC recipient's identity. 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 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.

Note: For workstations that are installed so that the card recipient faces the VO, the capability to rotate the fingerprint exists so that the fingerprint can be captured for the VO without physically moving the fingerprint reader to face the VO.

7. Select **Tools|Configuration**. Select the ***Readers*** tab and check **Rotate VO image**.

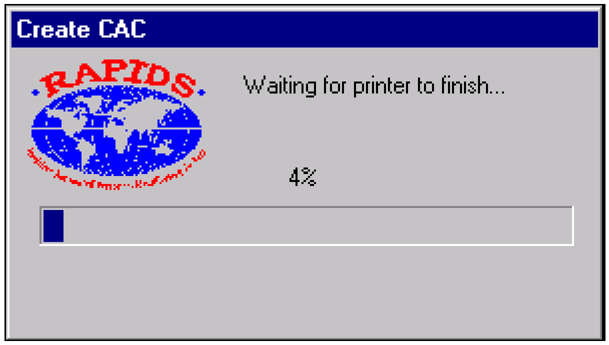
8. Take Photo.



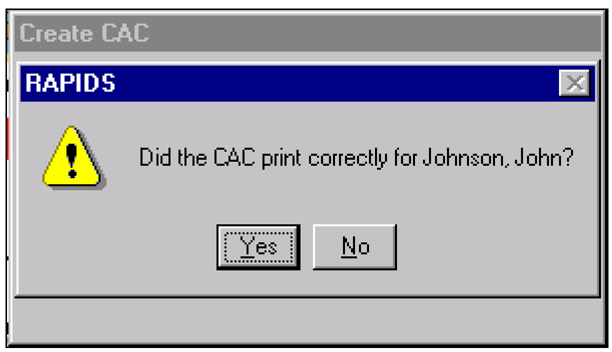
9. After taking the card recipient's photograph, the system will open the Print Card page of the Create Card Navigator. A preview of the CAC appears, as well as the request for the VO to enter the PIN. For security purposes, each CAC recipient must choose and enter a six to eight digit PIN. This PIN will be used to access personal entitlements, such as commissary and exchange privileges. This PIN should only be known by the cardholder. The card 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.

10. 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.

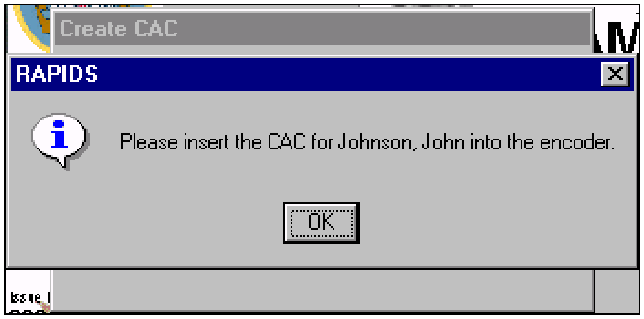
11. Ensure that the printer is ready and the CAC stock is properly loaded in the printer's feeder, and select the **Print** button.



12. 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 encoder/reader. Insert the CAC into the CAC smart card encoder/reader, chip up and chip first.



14. Encode the CAC. This process will 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 encoder/reader, two separate processes are completed. (1) Via a secure SSL session with the Issuance Portal/Hub, the ICC is encoded with personal data and associated applet. (2) Via a secure SSL session with the CA and Hub, the three certificates (identity, digital signature, and e-mail encryption) are created, issued, and encoded on the ICC with the associated applet. A progress meter displays to notify the VO of the portion of the automated process that is running. 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. The encoding process may seem to add to the process of producing the ID card; however, signing and laminating the card is no longer necessary. The increased level of security and additional coordination between systems account for the additional time.

15. Upon successful completion of encoding, leave the CAC in the smart card encoder/reader and follow the procedures detailed in *Section 6.5* of this Training Guide.

16. If the CAC recipient is also a VO, additional steps are required to add VO privileges. These steps are detailed in *Section 9* 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.

The photograph of the cardholder that appears on the CAC is in color.

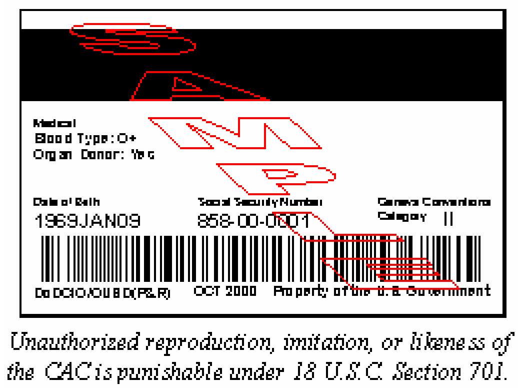
Front of CAC

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 Electronic Data Interchange Person Identifier (EDIPI), and Social Security Number (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
Branch of Service
Card Expiration Date
Card Issue Date
Card Security Code
Citizenship
Civilian Health Care Entitlement Type Code
Date of Birth
Demographic Date Chip Expiration Date
Direct Care Benefit Type Code
DoD Contractor Function Code
DoD EDIPI
Duty Status
Entitlement Condition
Exchange, Commissary, and Morale, Welfare, and Recreation (MWR) Codes
First, Middle, and Last Name
Gender
Government Agency
Meal Entitlement Code
Medical Benefits End Date
Name Suffix
Non-Government Agency
Non-medical Benefits End Calendar Date
Organ Donor
Pay Category
Pay Grade
PKI Functionality (3 certificates and private keys)
Rank
User PIN



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 and No. 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/OUSD(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.

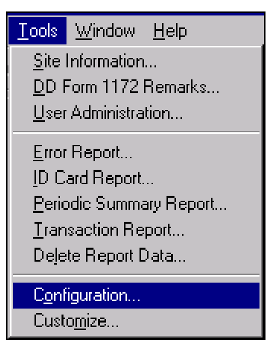
6.4.3 Certificate Revocation

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, RAPIDS will ask the VO to verify that the card has been destroyed. The VO should destroy the CAC by following the procedures for card return as detailed in **Appendix M** of this Training Guide.

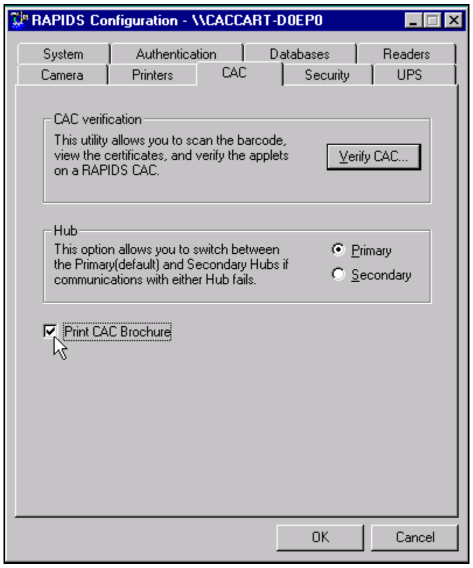
6.4.4 Verifying CAC Certificates

The VO should verify each CAC issued for certificates and inform each CAC recipient of the certificates encoded on his/her CAC.

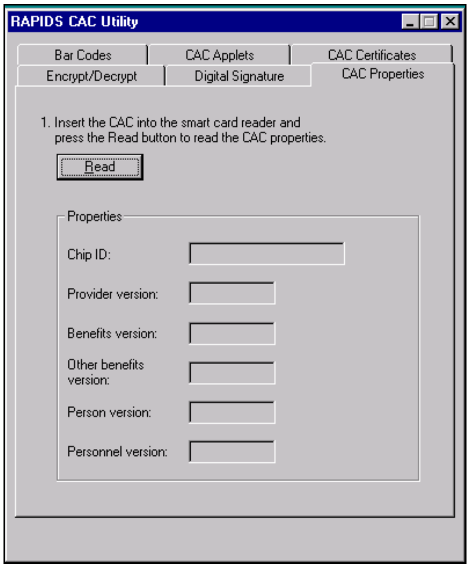
1. After printing and encoding a CAC, keep the CAC in the CAC smart card encoder/reader. Select **Configuration** from the Tools menu.



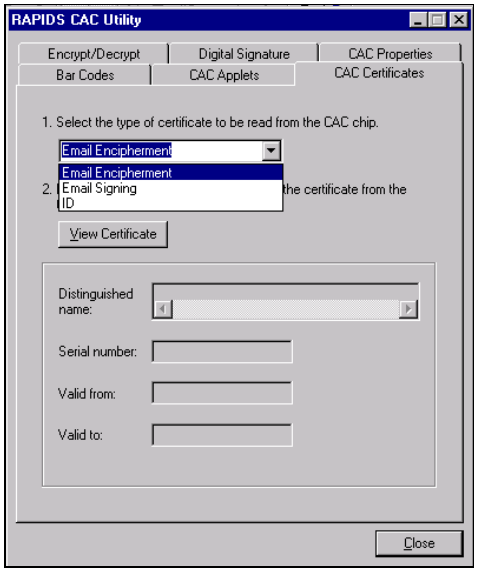
2. Select the ***CAC*** tab and click the **Verify CAC** button. Next, check to see if any certificates were encoded on the chip by selecting the ***CAC Certificates*** tab. Verify each certificate separately by highlighting a certificate and select **View Certificate**. The configuration screen refers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



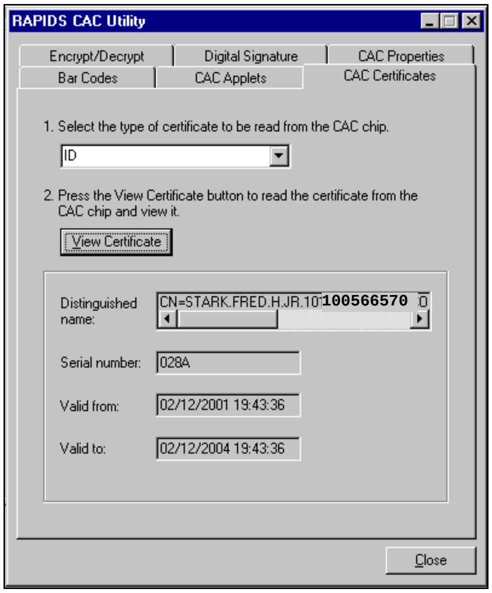
3. Select the ***CAC Properties*** tab and click on the **Read** button to check for CAC load. (This step is not required by the D/RPO but is useful in determining if the ICC is encoded).



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.



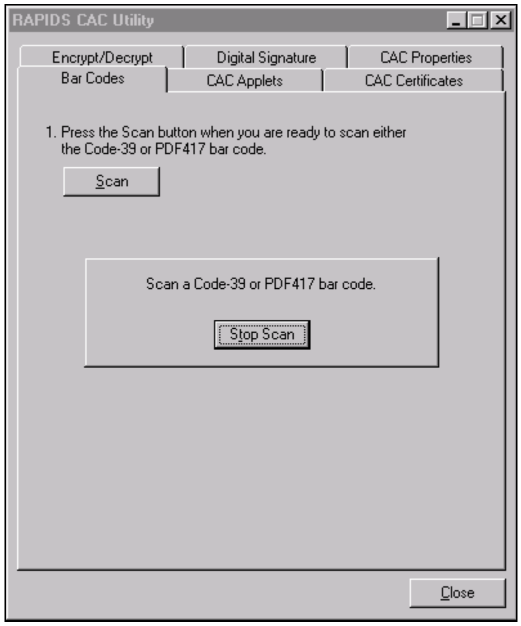
Note: Each certificate will populate the Verify CAC fields with a Distinguished Name, Serial Number, and Validation Dates.



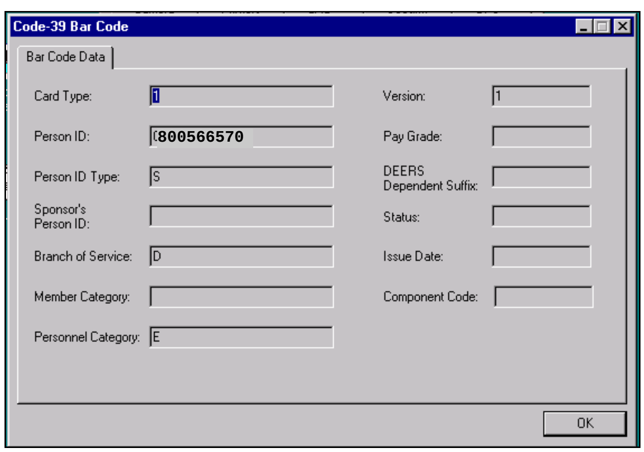
6.4.5 Code 39 Bar Code Testing

With the issuance of the CAC, other offices will begin to use the bar code imprinted on the CACs and the chip. It is more important than ever to ensure that the code 39 bar code (found on both the CAC and teslin cards) is readable. Effective with the receipt of RAPIDS 6.0 software, the VO is required to test the Code 39 bar code prior to giving the card recipient his/her newly created card. The VO should test the bar code by using the bar code scanner provided with the RAPIDS workstation.

1. After completing the certificate check, conduct a bar code check. Select the ***Barcode Tab*** and click the **Scan** button. For the slot scanner model, position the CAC at one end of the bar code scanner's slot with the Code 39 (one-dimensional) bar code facing the side with the lights and swipe it with a quick and fluid motion. For the laser scanner model, position the CAC with the Code 39 (one-dimensional) bar code facing up and align it under the scanner's laser beam, so that the red beam extends across the entire length of the bar code. For more details on how to use your model of bar code scanner, consult the RAPIDS Version 6 Hardware Guide, also found on this CD-ROM.



2. Verify card information from the Card Read dialog box. If a dialog box does not appear after the first scan attempt, visually re-inspect the bar code for obvious printing defects, ensure that the CAC is positioned correctly in the reader, and reattempt the bar code scan.

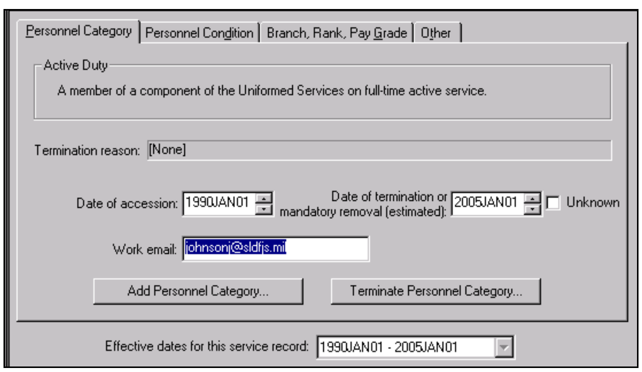


If the bar code does not scan, the VO should try to scan the bar code five to ten more times, ensuring the card is inserted into the scanner properly. If the bar code still can not be read and the site has more than one workstation, try another scanner. If the bar code is still not readable, issue another CAC and repeat the verification process. If the bar code still fails, the VO should report the hardware problem to the appropriate Support Center (D/RAC / DRSC-E / DSO-A) and allow the card recipient to leave with the CAC.

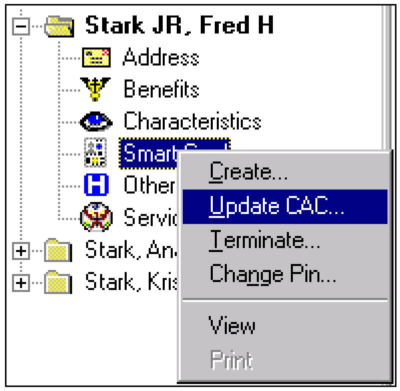
6.4.6 Updating a CAC

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 should be issued. 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. 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. During regular CAC issuance, a CAC may be updated when a sponsor's e-mail address changes.

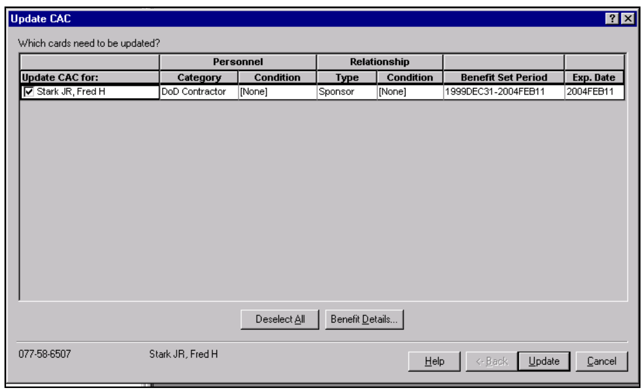
This segment details how to update a CAC. Under normal operations, this function is used after updating sponsor information that is not printed on the card. The most common reason for updating a CAC is to update e-mail certificates if an e-mail address changes.



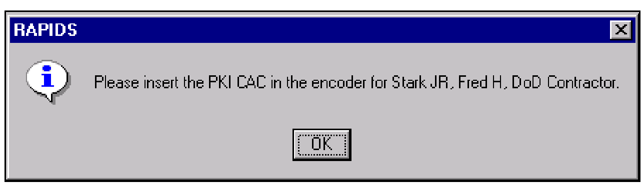
3. With the sponsor's record opened, right-click on the CAC ID Card and select **Update CAC** from the menu.



4. Select the sponsor from the Update CAC dialog box.



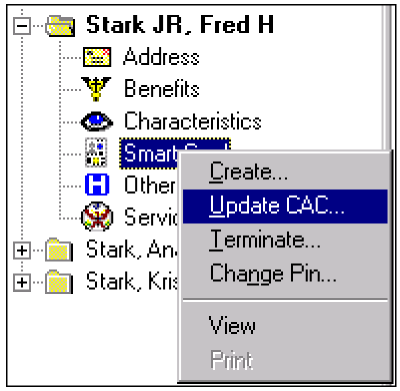
5. Ensure that the CAC is properly inserted into the reader. Click on the **OK** button to begin the Update process.



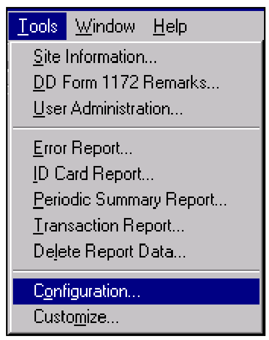
6.5 Troubleshooting for a CAC that Errors during Encoding

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 card. If an error occurs after a successful installation of the applets, the user will not be prompted to retry encoding.

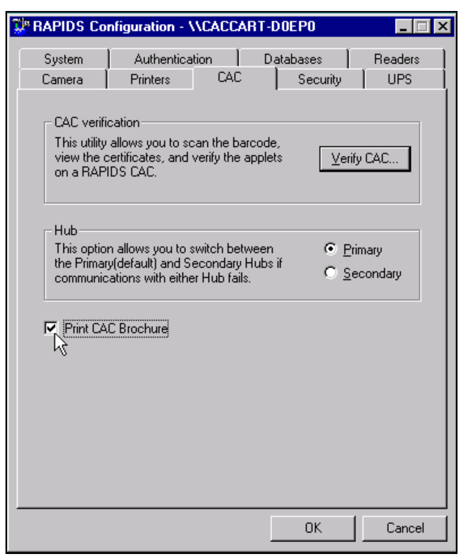
1. Use the “Update CAC” process (Select **Beneficiary|Card|Update CAC**) to reattempt encoding. Using the “Update” command is important because it does not remove data already written to the chip.



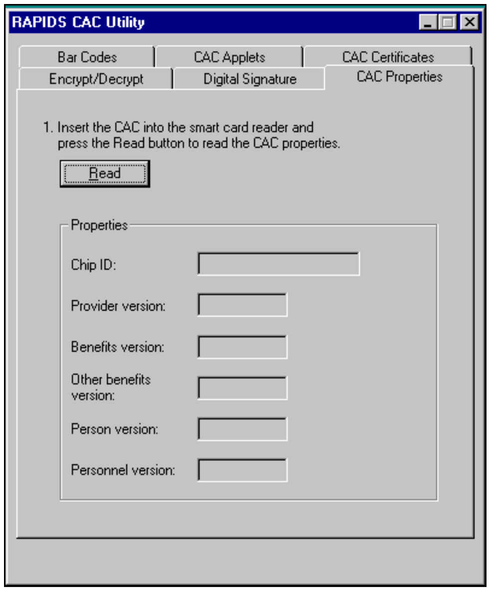
2. If updating fails, cancel out of the Navigator and open **Tools|Configure**.



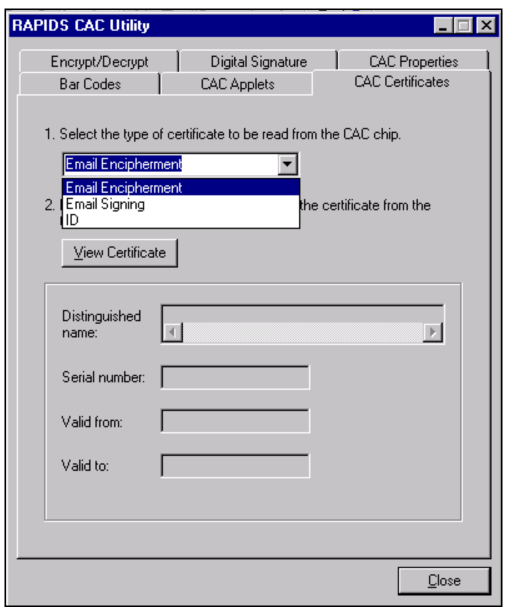
3. Select the ***CAC*** tab. Select the **Verify CAC** button.



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.



5. Next check to see if any certificates were encoded on the chip by selecting the "CAC Certificates" tab. Verify each certificate separately (E-mail Encipherment, E-mail Signing, and ID) 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 it is determined that the chip is faulty and it still cannot be encoded after the above attempts, then try a new card. If the card appears to have a bad chip, follow the CAC Destruction Process for Beta as outlined below.

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.

If the CAC is determined to be faulty, follow the CAC destruction procedures as detailed in this document.

6.5.1 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 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.

To physically destroy a terminated teslin card, the site personnel should follow the procedures in the AFI 36-3026. To destroy a CAC, site personnel should complete the Card Return Form **(Appendix M)** and return it with the CACs to the D/RAC.

All returned, terminated, defective, misprinted, non-encodable CACs should be returned to the D/RAC or appropriate Support Center using the form and instructions in **Appendix M** of this Training Guide.

6.6 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 also provides the following 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 encoder/reader. The card recipient must type the old PIN and type a new PIN two times for confirmation. PINs must be entered using the numeric keypad.

2. (The following option is unavailable during the Beta Test period). 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.

Note: All PIN maintenance transactions are audited.

6.7 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 Hub, 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.

6.8 Offline Processing

Offline processing occurs 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.

6.8.1 Offline Modes for CAC Production

For producing a CAC, different modes of offline exist because communication with three separate external servers (and communication with the RAPIDS server) is required to complete the CAC issuance: (1) DEERS database, (2) Issuance Portal/Hub, and the (3) 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. Consult the AFI 36-3026 and the RAPIDS VO CPS for the latest offline CAC issuance policies.

“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 10-280 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 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.

Return the sponsor's teslin card if it is not expired and have the customer return to receive his/her

CAC when communication has been reestablished.

6.9 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 form 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.

6.10 Smart Card 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.

DRPO/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. Forms will be provided to sites for **ordering additional CAC cardstock** when stock is low; however, sites will not be allowed to stockpile cardstock. The order processing center will also validate with DEERS that the site has actually produced the number of CACs related to the cardstock with which they have been provided thus far.

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 only handle the cardstock by the edges. 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 may be considered safeguarding.

CAC cardstock is issued to each eligible sponsor with an expiration date that is no longer than three years from the date of issue. The roll of laminate used within the printer is sufficient for 125 cards and 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. One cleaning card should be used. The same card can be used to clean the card feed assembly and the rollers.

6.10.1 Printer Ribbons, Laminate, and Toner Cartridges

DRPO/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. (Note: Each color printer ribbon can print 250 CACs, and each laminate roll can laminate 125 CACs, since only the top of the CAC.) An initial supply of CAC cardstock will be provided when the CAC-production hardware and software are installed at their site.

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

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 DRPO-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.

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 CAC printer ribbon destruction/disposal.

6.11 Temporary Identification Numbers and Foreign Identification Numbers

6.11.1 Temporary Identification Numbers

The RAPIDS software will issue a Temporary Identification Number (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 TIN will print in the family member's SSN field followed by the letter **D**. 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. Without connectivity to DEERS, the TIN cannot be generated and the ID card cannot be issued for the family member without an SSN.

6.11.2 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 FIN for this category. When prompted to type in the Sponsor's Identifier, the VO should select **Foreign Identification Number** from the drop down menu in the Open Family dialog box. DEERS will generate a unique FIN for these individuals. Foreign National employees who will be working as RAPIDS VOs, SVOs, or SSMs should also have a FIN generated for them. As with TINs, when offline, sites do not have the capability to generate a FIN and issue an ID card for a Foreign National.

6.12 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.

6.12.1 Site Information

To modify your RAPIDS site address and/or UIC, click the "Modify Site Info" button within this option. To ensure consistency and accuracy of site information, all RAPIDS Site Name or Telephone Number change requests should be routed through the appropriate DEERS/RAPIDS SPOs listed in Appendix C.

6.12.2 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 5.x.

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.

6.12.3 Refresh DEERS Data

This option should only be selected when instructed by the D/RAC, D/RSC-E, or DSO-A. A warning will appear, informing the user that this procedure may take over five minutes, depending on the quality of communications.

6.12.4 User Administration

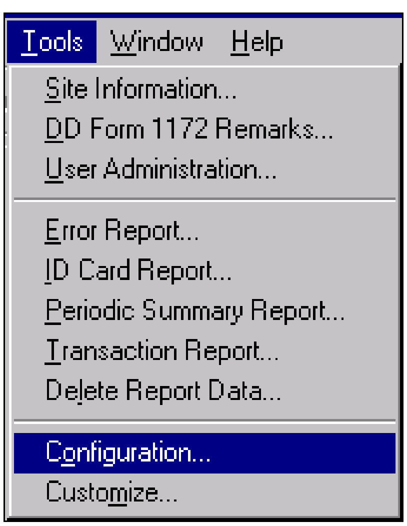
This option is detailed in *Section 9* of this Training Guide.

6.12.5 Reports

These options are detailed in *Section 8* of this Training Guide.

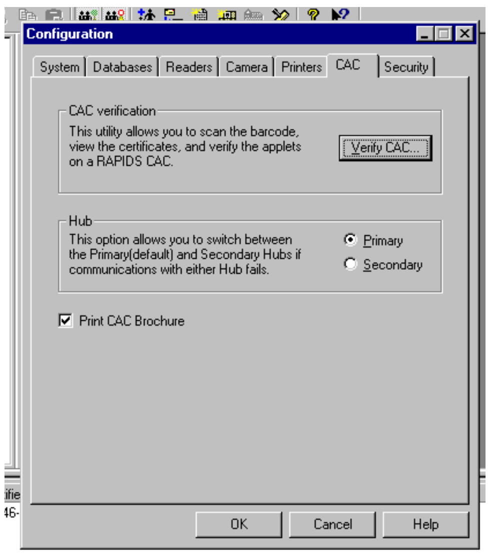
6.12.6 Configuration

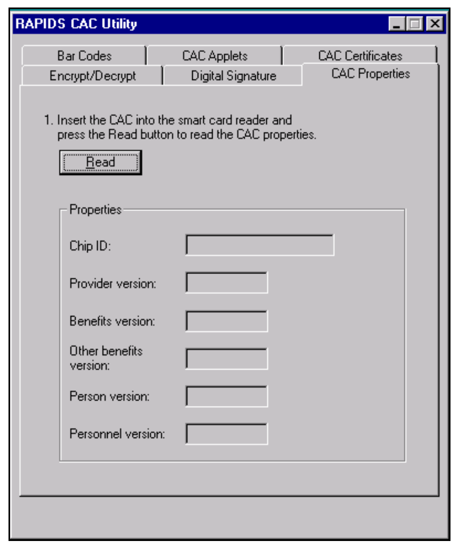
The Configuration tool is used to obtain information **via *System, Authentication, Databases, Readers, Camera, Printers,*** and ***CAC*** tabs. All users can view the Configuration option. Updates are restricted to RAPIDS SSMs under the direction of the D/RAC / D/RSC-E / DSO-A.



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 encoder/reader. Select the **Verify CAC** button to view the following additional tabs.

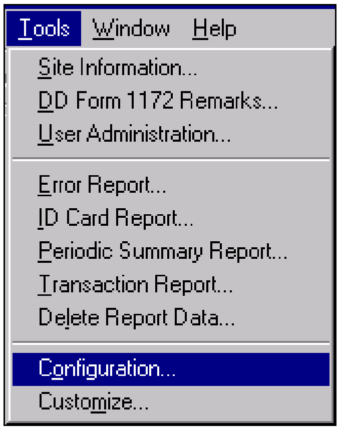
- The ***Bar Codes*** tab allows the VO to scan either the Code 39 or PDF417 bar code.
- The ***CAC Applets*** tab allows the VO to read benefits, person, or personnel information from the CAC chip when inserted into the reader.
- The ***CAC Certificates*** tab allows the VO to read the E-mail Encipherment, 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.

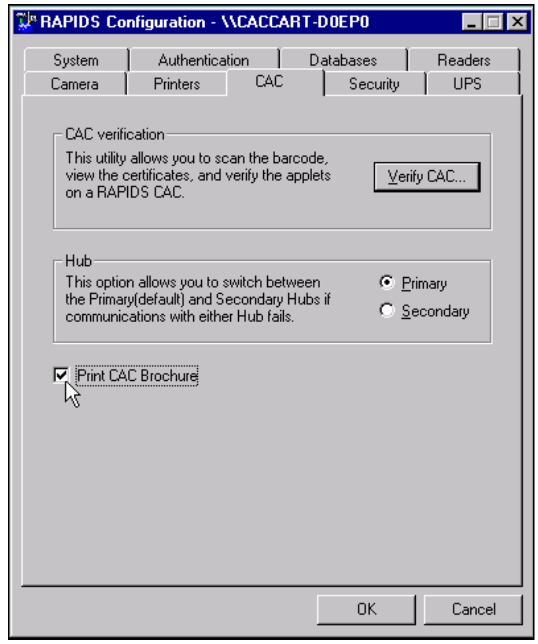




6.12.7 Printing the CAC Brochure

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 by selecting **Tools|Configuration** from the menu.





Select the *CAC* tab from the RAPIDS Configuration screen. Check the **Print CAC Brochure** box to enable.

6.12.8 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.

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 a particular VO.

6.13 RAPIDS Site Locator

To access the RAPIDS Site Locator to locate RAPIDS ID card offices (using a PC with Internet access), use the following procedure.

1. Select and open Microsoft Internet Explorer or another World Wide Web browser.
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. This application is used to find the locations of ID card offices.

6.14 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.

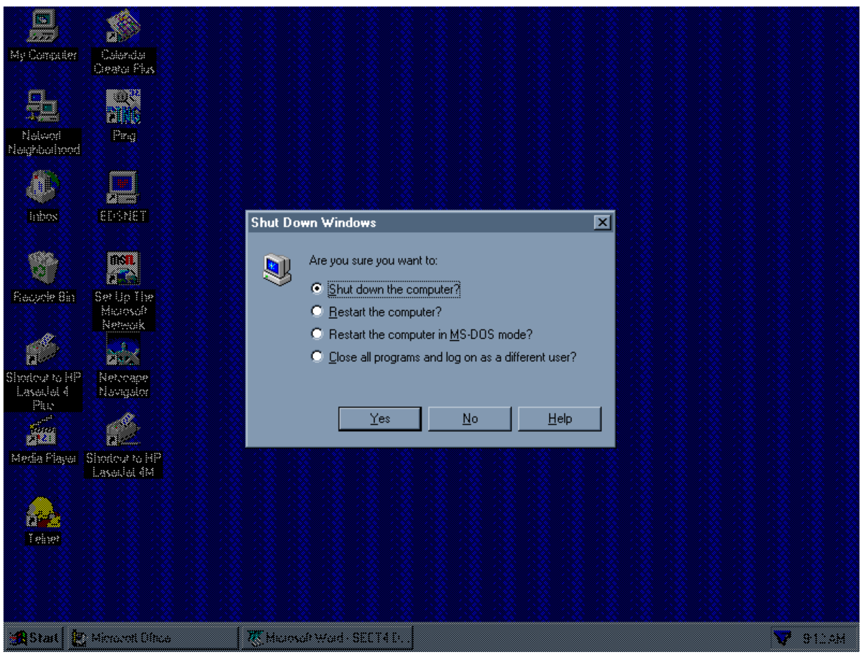
6.15 Screen Printing through RAPIDS and Windows

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

1. At the desired screen, press PRINT SCREEN (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.

6.16 Quitting Windows NT 4.0

Quitting Windows NT 4.0 is a fairly simple task. Never turn off your computer while RAPIDS or Windows NT 4.0 is still running. Properly shutting down the system allows the temporary information stored in memory to be saved to the hard drive. After you have quit RAPIDS by selecting **File|Exit** from the main menu and disconnecting your communications to the RAPIDS server, you may then proceed to shut down Windows NT 4.0. You can shut down the operating system by clicking **Start** from the taskbar and selecting the **Shut Down** command. A dialog box entitled Shut Down Windows appears. To completely shut down the system, select **Shut down the computer?** and click **Yes**. To logoff so that another user can log in, select the option **Close All Programs and Login As A Different User**. If you choose the **Shut Down** option, your computer will display a screen telling you when it is safe for you to shut off your computer. Turn off your computer, monitor, and peripherals via the surge suppressor switch.



Windows NT 4.0 Shut Down Window

Note: NEVER shutdown 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 server disables any of the connected RAPIDS workstations from using RAPIDS in either online or offline mode.

7 Training Scenarios

7.1 Introduction

This chapter will illustrate 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 5* of this Training Guide to assist you.

7.2 Add a New Family to DEERS

1. Select the **New Family** command from the **File** menu or the toolbar button.
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.

7.3 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.

7.4 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.

1.1 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, the VO should 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.

1.2 Update a Military Sponsor's Marriage Status to Reflect a Joint Service Marriage (JSM)

1.2.1 JSM Sponsorship

1. Open first Sponsor.
2. Open **Characteristics** view.
3. On the ***Sponsor Specific*** tab, place a check mark in the **Joint Service Marriage** checkbox and enter Spouse's Identifier.
4. Select the Save Family  icon from the main toolbar.
5. Repeat steps 1-4 with other Sponsor's (spouse) information.

Note: Family Members may not be enrolled to receive the same benefit (s) under more than one sponsor. In some instances a family member (s) may be enrolled under two sponsors so long as the family member (s) will not be eligible for the same benefit under both sponsors.

1.2.2 Update a JSM Sponsor to Become a Dependent Spouse under the Other Sponsor's Record

Note: 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:** one member retires and becomes a dependent under the other Active Duty record.
- **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 Sponsor who is retiring or separating.
2. Open **Characteristics** view.
3. On the ***Sponsor Specific*** tab, deselect the checkmark for **Joint Service Marriage** and ensure the marital status reflects Married.
4. Update the sponsor's **Service Record** view to reflect retired, terminated, or separated (according to the documentation).
5. Select the Save Family  icon from the main toolbar.
6. Open Sponsor's record to which the spouse needs to be added as a dependent .
7. Open **Characteristics** view for the sponsor.
8. Select ***Sponsor Specific*** tab.
9. Deselect the checkmark for **Joint Service Marriage** if it has not already been updated. Ensure marital status reflects Married.
10. Add spouse to the record. (Refer to Section 7.3). 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.
11. To correct the benefits start date, open the spouse's **Characteristics** view.
12. On the ***Relationship Condition*** tab, click **Add Relationship Condition**.
13. 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**.
14. On Summary, select **Finish**.

Note: Steps 10-14 erase all benefits associated to the spouse's record prior to the actual start date of the spouse dependency. The Benefits view will now reflect the start date of benefits as the dependent spouse's retirement date or one day after the separation or termination date.

7.6.3 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 7.3).

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.

7.7 Divorce a Sponsor from a Spouse Who Does Not Meet Unremarried Former Spouse (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. 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 Unremarried Former Spouse (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.

7.8 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.

7.9 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 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.

7.10 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.

7.11 Update Active Duty Sponsor to Temporary Disabled Retirement List

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 Temporary Disabled Retirement List (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 (DoDI 1000.13 and AFI 36-3026).

7.12 Update TDRL Sponsor to Permanently Disabled Retired List

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 for Permanently Disabled Retired List (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.

7.13 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 Separation Program Designator (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.

7.13.1 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 Separation Program Designator (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.

7.13.2 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.

7.14 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 Summary, select **Create**. A Guard/Reserve card can now be issued.

11. Select the Save Family icon from the main toolbar.

7.15 Separate Sponsor and Issue Transition Assistance, Voluntary Separation Incentive, or Special Separation Benefit 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 Transition Assistance (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.

7.16 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 with correct medical dates to establish commissary, exchange, and MWR privileges.
4. Re-take the photograph and select **OK**.
5. On Summary, select **Finish**.
6. Print ID card.

7.17 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 and select the Save Family  icon from the main toolbar.
4. 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.

7.18 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 (such as Bosnia or Kosovo), select the condition of Activation for Special Operation with the specific operation selected in the navigator.
5. On Summary, select **Create**.

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.

7.19 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 and select the Save Family icon from the main toolbar.
4. Proceed to DD Form 1172 and ID Card Navigators to issue new DD Form 1172 and ID card.

7.20 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**. 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. Select the Save Family icon from the main toolbar.

7.21 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.

7.22 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**.

7.23 Separate Guard/Reserve Sponsor from an Active Duty Mobilization (TA-30)

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-30 card can now be issued.
7. Select the Save Family  icon from the main toolbar.

7.24 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.

7.25 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: URFS of Reserve retirees are not entitled to benefits until the sponsor reached age 60.

7.26 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.

7.27 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 60th birth date in Retirement Date. Select **Finish**.
5. On Summary, select **Finish**.

6. Select the Save Family  icon from the main toolbar.

7.28 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.

7.29 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.

7.30 Medicare

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 terminate CHAMPUS benefits based on the person's age and Medicare rules. RAPIDS collects Medicare information that is an exception to the default.

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 are 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.

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

Medicare Part A Reason Codes include:

- 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.

Medicare Part B Reason Codes include:

- Enrollment in Part B under age 65 - When entering this value the system is being told that the individual has purchased Medicare Part B prior to the individuals Medicare Eligibility date. The effective date of this Medicare Part B must be before the individuals Medicare Eligibility date and end one day prior to the Medicare Eligibility date.
- Enrollment in Part B on or over age 65 - When entering this value the system is being told that the individual has enrolled in Medicare Part B after or on the individuals Medicare Eligibility date. The effective date of this Medicare Part B must be on or after the individuals 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 CHAMPUS starting at his Medicare Eligibility date.   Once a Medicare Part B “Enrollment in Part B on or over age 65” is added CHAMPUS eligibility as a secondary payer is returned to the individual for the duration of the Part B segment. Note: CHAMPUS 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 CHAMPUS for the entire duration of the Part A segment.
- Medicare Part A Reason “Eligible after 65th Birthday” – The individual loses eligibility to CHAMPUS during the duration of the Part A.   Once a Medicare Part B “Enrollment in Part B on or over age 65” is added CHAMPUS eligibility as a secondary payer is returned to the individual for the duration of the Part B segment. Note: CHAMPUS 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 looses eligibility to CHAMPUS during the duration of the Part A. Once a Medicare Part B “Enrollment in Part B under age 65” is added CHAMPUS eligibility as a secondary payer is returned to the individual for the duration of the Part B segment. After age 65 a Medicare Part B “Enrollment in Part B on or over age 65” can be added and CHAMPUS eligibility as a secondary payer is returned to the individual for the duration of the Part B segment. Note: CHAMPUS 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 CHAMPUS for the entire duration of the Part A segment.
- Medicare Part B Reason “Enrollment in Part B under age 65” with no corresponding Part A enrollment - The individual remains eligible for CHAMPUS for the entire duration of the Part A segment.
- Medicare Part B Reason “Enrollment in Part B on or over age 65” ” with no corresponding Part A enrollment – When over 65 and individual is either eligible for Medicare Part A or not. When there is no Medicare Part A segment for a particular span of time the default rule is applied. After adding the Medicare Part B “Enrollment in Part B on or over age 65”, CHAMPUS eligibility as a secondary payer is returned to the individual for the duration of

the Part B segment. Note: CHAMPUS 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 CHAMPUS regardless of their enrollment in Medicare Part B. See the Service Regulations for details.

7.30.1 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. 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 dually entitled for Medicare and Civilian Health), enter **Medicare Part B** (Enrollment in Part B Under Age 65) 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.

7.30.2 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. Select **Finish**.
5. On Summary, select **Finish**.
6. Select the Save Family  icon from the main toolbar.

7.30.3 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. Select **Finish**.
5. On Summary, select **Finish**.
6. Again, click **Add Medicare**.
7. Enter **Medicare Part B** (Enrollment in Part B on or over age 65) 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.

7.31 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.
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 60th 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

13. Select **New Family** from the **File** menu.
14. Type the sponsor's identifier and select **Enter**.
15. 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**.
16. Enter the sponsor's name and marital status. Select **Next**.
17. Enter the date of birth, gender, and physical attributes. Select **Next**.
18. 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**.
19. Enter the sponsor's home address, phone number, and home e-mail address with effective dates. Select **Finish**.
20. 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 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, Agency/Subagency, and DoD Contract type. Select **Next**.
7. Enter the pay category and Geneva Conventions category. Select **Next**.
8. Enter the sponsor's home address, phone number, and e-mail address with effective dates. Select **Finish**.
9. On Summary, select **Create**.

Note: Family members should not be added to DEERS unless receiving 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, 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 will also receive 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 7.3 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).

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. The field will populate with zeros.

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, 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 7.3 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

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

Note: Contact your SPO in all cases of dependent abuse. Only the SPO can make the necessary modifications to the Sponsor's record to ensure that the dependents receive the privileges to which they are entitled. The SPO can also advise on whether the dependents meet the eligibility criteria for obtaining the DD Form 1173. The DD Form 2698 should be forwarded to the SPO to ensure that the sponsor’s and family members’ RAPIDS records correctly reflect 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. 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 s 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, select **Relationship Condition**, and enter **Transitional Compensation on AD** or **Transitional Compensation for Ret**. The description should read "Enter *DD Form 2698 Application For Transitional Compensation.* Block 21a & b Start and Stop payment dates for family members whose sponsor was on Active Duty for more than 30 days. For family members whose sponsor is retirement eligible, enter the Start date and Stop date as reflected on the DFAS-CL letter or enter Unknown.

   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."
5. Select **Finish**.
6. Select **Save**.

7.43 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.
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. Enter the number of years of marriage, the sponsor's length of service, and the number of years marriage that overlaps with the sponsor's years of service. Check **Eligible for Transition Compensation**.
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.

7.44 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.

7.45 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.

7.46 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.

7.47 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.

7.47.1 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.

7.47.2 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.

1. Do not pull the cardstock through the rollers. Allow the cardstock to feed through the printer at its own pace.
2. 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.

7.47.3 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

8.1 Introduction

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.

8.2 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.

8.3 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 or telephone 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.

8.4 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.

8.5 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.

8.5.1 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.

8.5.2 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.

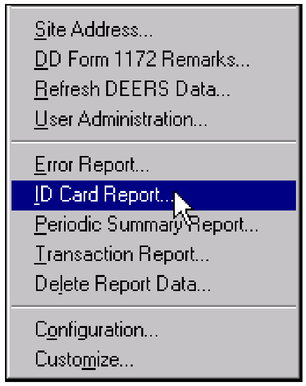
8.5.3 ID Card Report

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

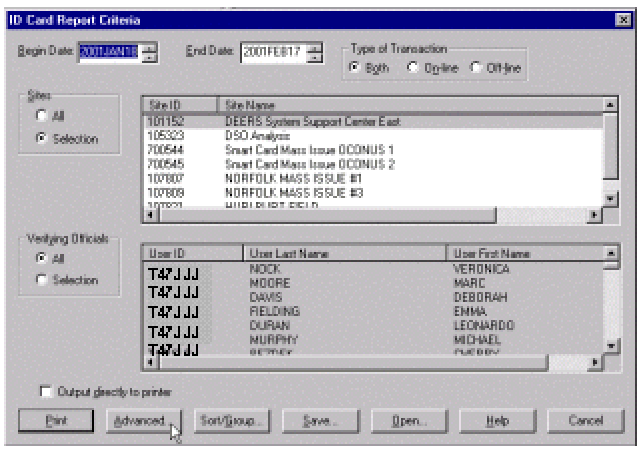
1. Select **Tools** from the main menu.
2. Select **ID Card Report** from the drop-down list to display the ID Card Report Criteria dialog box.
3. Type the beginning and ending dates for the report.
4. Select **Transaction Kind**, **site ID**, and **Verifying Official(s)** as needed.
5. The ***Advanced*** 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.

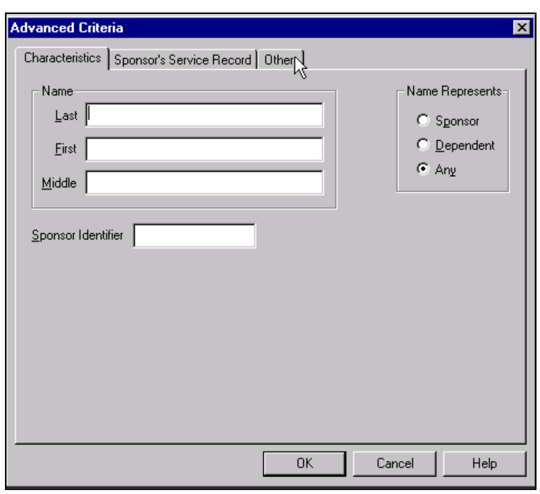
1. Select the ID Card Report from the Tools Menu.



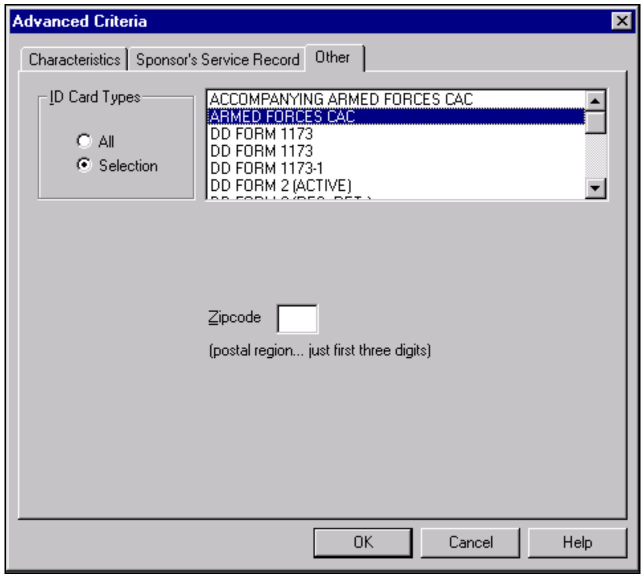
2. Click on Advanced to select the Card Type to report on.



3. Select the ***Other*** Tab.

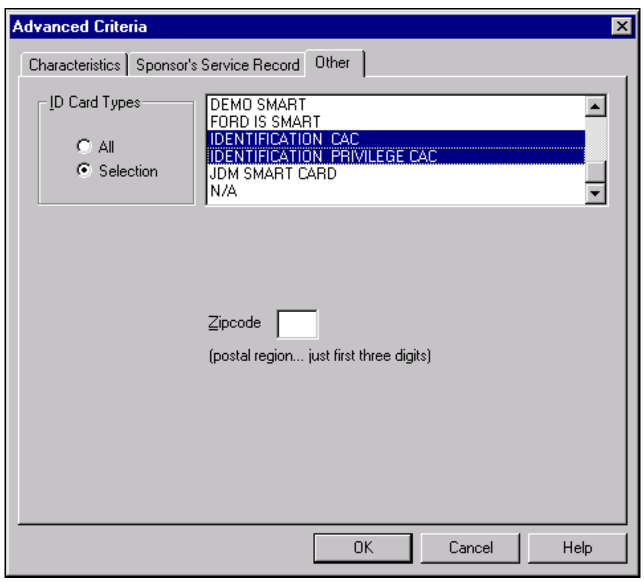


4. From the Other tab of the Advanced Criteria, select the **Selection** radio button, then choose the appropriate CAC option from the list.



Depending on the site, the options may include:

- Armed Forces CAC
- Identification CAC
- Identification Privilege CAC



5. When complete, click on the OK button. The report will be generated. Print the report and follow the Beta Test Reporting Procedures as explained earlier in this document.

8.5.4 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.

8.5.5 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.

8.5.6 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 ½" 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.

8.5.7 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 SVOs. 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.

No hard requirement was established for generating the RAPIDS reports and deleting the report data from the RAPIDS server. FSRs have suggested these reports be run at least monthly, to include deleting the data after printing the reports. 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. All RAPIDS SVOs should run the reports at least monthly and delete the information that is no longer needed. For assistance in printing and deleting reports, contact your FSR or the D/RPO / D/RSC-E / DSO-A as listed in **Appendix** *A* or *B*.

9 Using RAPIDS SSM Functions

9.1 Introduction

This section will explain RAPIDS functions for use only by users with the SSM role.

9.2 User Administration

With the advent of CAC issuance with PKI certificates, VOs will now need a higher level of security and will be added as special users to the CAC and corresponding directories. The VO requires a certificate allowing him/her to request the generation of other CAC recipients' certificates.

1. 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 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.
2. 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 previously using RAPIDS 5.2; however ALL users will need to have LRA certificates updated.

Only the RAPIDS SSM for a specific site will have access to the User Administration option within **Tools**. The SSM will have the ability to request new login IDs, activate existing login IDs, update users with LRA privileges, assign roles, update user information, reset passwords, and delete users. The RAPIDS SSM also has the capability to update the site's address by selecting **Tools|Site Address**.

To use the RAPIDS application that accesses the DEERS database, the VO must insert his/her CAC into the VO card reader. When the login screen appears, the VO must type the PIN associated with his/her CAC in the Access Card Gold login screen to access Windows NT. When RAPIDS is started, the Windows NT login information is compared to the login ID and password stored on the server's local database to verify the user is authorized to run RAPIDS. This stored login 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. <u>This password is stored on the local server and is used by the application anytime a DEERS record is requested.</u>

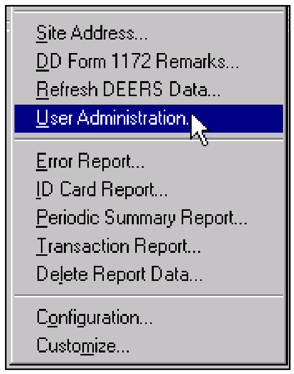
For security purposes, neither the password nor the PIN should be shared with anyone, including other VOs, the SVO, or the RAPIDS SSM. For additional system protection, neither the login ID password nor the PIN is saved on the login screen. The PIN will not be displayed on the screen as it is typed.

As part of the login 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 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.

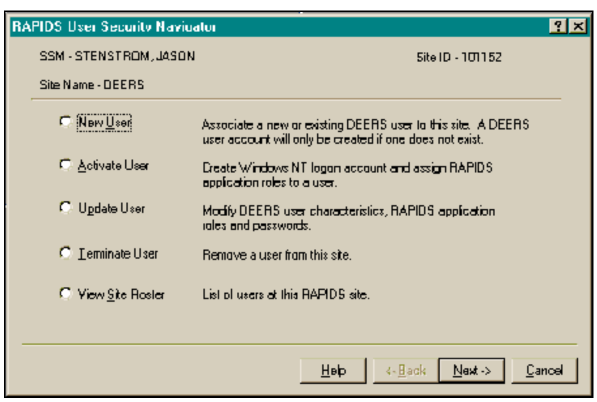
9.2.1 Add New User

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

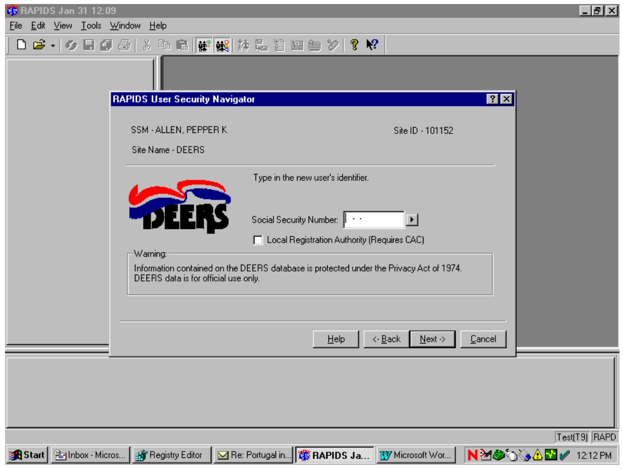
1. Select **Tools|User Administration** from the main menu.



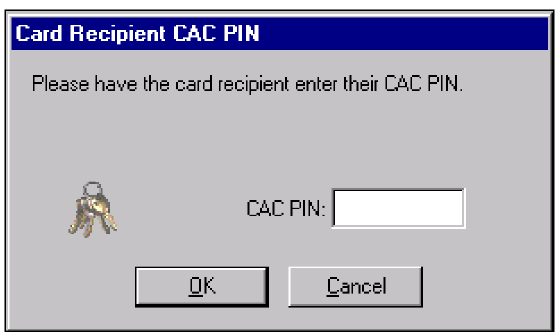
At the RAPIDS User Security Navigator**,** select **New User** and click **Next**. This action associates a new or existing DEERS user to this site. A DEERS user account will only be created if one does not exist.



2. The SSM logged into RAPIDS should have his/her CAC in the VO reader**.** Insert the new user's CAC into the card recipient's encoder/reader and check the box for "Local Registration Authority (Requires CAC)."



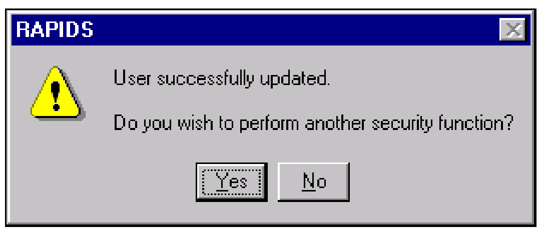
It is not necessary to input the Person Identifier if the CAC is inserted. The VO should be prompted for their PIN. An "Update User" progress monitor will appear with a status detailing that DEERS is being updated. When prompted, the card recipient should enter his/her CAC PIN (six to eight digits).



If the VO is already an existing VO, DEERS will return a message stating the same.

3. DEERS will return the DEERS Security dialog box. Enter or confirm the information requested. Select Finish.

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 will be added to the LRA security table and will be able to conduct VO functions on a RAPIDS 6.0 workstation. The newly updated RAPIDS user will not be able to log in to RAPIDS using his/her CAC until the following business day.

Issuing a CAC to an individual that is a VO does not enable that VO to perform VO functions under a RAPIDS 6.0 workstation. After the VO is updated, following the steps listed, the VO must then register their CAC on each RAPIDS 6.0 workstation and set their NT Login Account for the RAPIDS 6.0 server. Follow the procedures detailed in *Section 5* of the RAPIDS Training Guide.

The login ID and initial password will be generated overnight for new users. On the following business day, the RAPIDS SSM should activate the user and assign the appropriate roles for the new user(s). A form will be mailed to the newly added user with the new login ID and password.

9.2.2 Activate User and Assign Roles

RAPIDS users may have more than one role at any given time (i.e., VO, IO, SVO, and SSM). Users with multiple roles will not have to logoff and login 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 login ID and initial password from the DEERS Security Office.

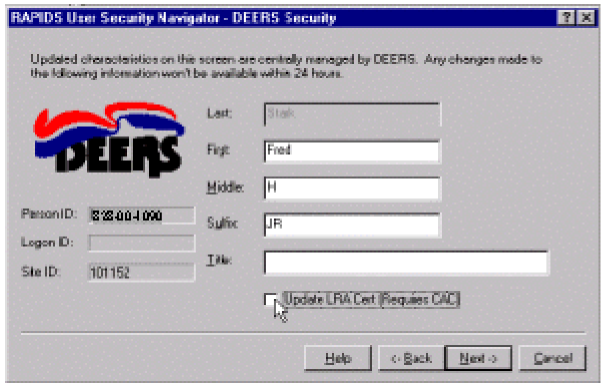
1. Select **Tools|User Administration** from the main menu.
2. At the RAPIDS User Security Navigator, select **Activate User** and click **Next**.
3. Select the user you wish to activate, and click **Next**.
4. Input the pay grade and phone number, and enter the DEERS password. Click the desired role 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.

1. If a new CAC is issued or if information changes on a VO, these processes need to be repeated with the newly issued CAC. Select **Tools|User Administration** from the main menu.
2. At the RAPIDS User Security Navigator, select Update User and click **Next**. Select the user for which you wish add LRA privileges or update.
3. Insert the CAC for the VO you wish to update into the card recipient’s encoder/reader and 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.



4. 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.

5. Select **Finish**.

9.2.4 Terminate Users

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

From time to time a RAPIDS SSM may need to see a list of DEERS/RAPIDS users at his/her site. The SSM should follow these steps to view all 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 Using RAPIDS Configuration Utilities

The RAPIDS Configuration Utilities application can be accessed in the following two ways.

1. Select the RAPIDS Configuration Utilities icon on the Windows desktop.

   -or-

2. Select **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* for detailed instructions on using the CAC options.

9.4 RAPIDS Software Distribution

The ideal way to distribute new versions of RAPIDS software is to make the upgrade transparent to the user. The intent is to download it through the communication links using an automated software distribution package. Software distribution may also be performed by sending out CD-ROMs, floppy disks, or through electronic file transfers until the automated software process is complete.

10 Deployable RAPIDS

Note: This section describes Deployable RAPIDS, Version 5.2. This section of the Training Guide will be updated as future versions of Deployable RAPIDS become available. RAPIDS 5.2 does not support issuance of the CAC.

10.1 Overview

Deployable RAPIDS is a laptop version of RAPIDS used in mobilizations or on ships. It is the same software and behaves identically to the desktop RAPIDS when online. Differences are experienced when offline or “deployed.” This section is to be used only for RAPIDS hardware configured as Deployable hardware. When RAPIDS is loaded onto a deployable workstation such as a laptop, it looks and feels like RAPIDS on a desktop 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 an offline mode called deployed mode for extended periods.

This section is designed to teach users the different features of deployable RAPIDS. The section is organized in the following manner.

1. Before your unit deploys…(READ NOW!)
2. Hardware overview: Setting up deployable RAPIDS
3. Establishing communications on deployable RAPIDS
4. Deployable user administration
5. Logging on to deployable RAPIDS
6. Creating ID cards using deployable RAPIDS
7. Deployable Data Storage and Transmission

10.2 Before Your Unit Deploys… (Read Now!)

To ensure that you can use deployable RAPIDS quickly and easily, we recommend that your unit take the following steps well in advance potential or actual deployment.

1. Read this entire section carefully with all your deployable hardware in front of you. Note any questions. 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**).
2. Take a paper copy of the RAPIDS Training Guide with you on a deployment. Remember, Online Help will not be available to you until you can successfully boot up the laptop.

3. If provided, read the manufacturer's user instructions for the hardware that has been issued to your unit. The hardware information provided in this section is not designed to be a complete set of instructions. Make sure any manufacturer's instructions are kept with the deployable RAPIDS.

4. Try using your deployable RAPIDS both with and without communications before you deploy. This will promote training, teach you what resources you need in order to use deployable RAPIDS, and ensure that you follow the necessary steps. The goal is to utilize deployable RAPIDS with confidence.

10.3 Hardware Overview: Setting Up Deployable RAPIDS

Though deployable RAPIDS is designed to be packaged and shipped together as a single unit, someone in a deployed unit must learn how to identify and assemble the components prior to using the system and how to disassemble and repack the system in the soft-sided carrying cases after using the system. .For more detailed information on the deployable hardware, please refer to the "RAPIDS Hardware Guide and manufacturer documentation provided with your deployable RAPIDS system.

10.3.1 Deployable RAPIDS Components List

This list reflects the hardware that is officially supported by the initial 1999 rollout of deployable RAPIDS.

- **Laptop Computer:** Panasonic Toughbook CF-27 with AC adapter/charger and power cord
- **Digital Camera:** Apple Quick Take 150, Kodak DC220, or Kodak DC265 with interface cable, AC adapter, power cable, batteries, and battery charger
- **Laser Printer:** Hewlett Packard (HP) LaserJet 5L, LaserJet 5L-FS or LaserJet 1100 with toner cartridge (in nylon bag), power and interface cables
- **Laminator:** National Laminating 5000T
- **Surge Suppressor:** American Power Conversion (APC) 7 outlet Surge Arrest or Belkin 8-outlet Surge Master II
- **PCMCIA Communications Cards:** 3Com Personal Computer Memory Card International Association (PCMCIA) Combination Modem/Ethernet Network Interface Card (NIC)
- **Fingerprint Scanner:** Identicator DFR-90 with power and interface cables, parallel port dongle, PreScan pad and cleaning cloth.
- **PCMCIA Framegrabber Card:** MRT VideoPort Professional PCMCIA card and interface cable with RCA/BNC adapter on the end.
- **USB Hub:** Inside Out Networks Edgeport/421 with USB interface cable provides four additional USB ports, two serial ports and one parallel port.
- **CD-ROM Drive & Floppy Disk Drive External Cable:** The Panasonic laptop comes with a CD-ROM drive installed and external floppy disk drive with parallel interface cable.

- Laptop Computer and Laser Printer Soft-sided Carrying Cases with Plastic Cardstock Case and Nylon Toner Bag
- Deployable System Dust Cover

The following are optional deployable RAPIDS components; not every system will have these items.

- Laptop Computer Hard-sided Transit Case
- Laser Printer Hard-sided Transit Case

Other optional peripherals, such as bar code scanners, plastic smart card printers, smart card reader/writers, PIN keypads, and soft-sided smart card printer carrying cases may be added to deployable RAPIDS.

10.3.2 Connecting Components

To assemble and set up deployable RAPIDS, ensure that all items have been received by unpacking both soft-sided carrying cases and checking the contents against the packing list in the cases.

The following rules will enable you to connect all the components of deployable RAPIDS.

1. **Match connector shapes!** It is not a prerequisite to know how to recognize a parallel from a serial port. What is necessary is to put round pegs into round holes, long skinny rectangular pegs into matching holes, and so on. The deployable laptops have a limited number of holes or "ports," so if you remember that the shapes must match, finding the right port for each component's adapter should be easy.

2. **Connect peripheral devices and turn on before starting up the laptop.** During the boot-up process, a computer recognizes any peripherals that are attached to it. To guarantee that the laptop can "talk" to them, they must be connected to the laptop and turned on, before turning on the laptop computer. One exception is the camera; it can be connected to the computer at any time.

10.3.2.1 Power Connection and Requirements

The deployable system components run on 110 Volts (V), 50/60 Hertz (Hz) power. All components with a power cable should be plugged into the surge suppressor and the surge suppressor plugged into an alternating current (AC) power outlet or generator.

If you are without power for an AC wall outlet or a generator, you may still use deployable RAPIDS for limited periods of time for non-printing functions. The laptop has an internal battery and spare battery that can be recharged when installed in the laptop while it is plugged in. Each battery, depending on its charge level, may give you two or more hours of use. The deployable camera can also function using its AC adapter or can draw power from batteries. The laser printer, laminator, and fingerprint scanner must be plugged into an AC wall outlet or generator power source in order to function. Be sure to plug all items using AC power into the surge suppressor, and plug the surge suppressor into the AC wall outlet or generator to prevent any damage to deployable RAPIDS components.

10.3.2.2 System Assembly

To assemble and set up the deployable RAPIDS system, perform the following steps.

1. **Laptop Computer:** Connect the laptop's AC adapter/power cable between the laptop and the surge suppressor. All other connections to the laptop are discussed for each piece of hardware listed below. For details on connections see figures in *Section 10.3.3*.

2. **CD-ROM and External Floppy Disk Drive Cable:** The laptop will arrive with the CD-ROM drive installed, and the floppy drive can be attached to the printer port on the back of the laptop using the supplied cable. For normal RAPIDS operations, the floppy disk drive should be installed in the device bay and the CD-ROM drive should not be used, except during software installation.

   Note: You cannot connect/use the printer with the floppy disk drive connected to the printer port.

3. **Laser Printer:** Plug the dongle that comes with the fingerprint scanner between the laptop's printer port and the printer's interface cable. Connect the laser printer's interface cable between the back of the printer and the printer port on the back of the laptop. For deployable sites using the smart card printer, the smart card printer is plugged into the laptop's printer port while the laser printer is plugged into the USB hub. Connect the power cable between the printer and the surge suppressor. Install the toner cartridge (in nylon bag) in the printer, according to the instructions provided in the printer's manual.

4. **Digital Camera**

   a. **Apple Quick Take 150:** Connect the camera interface cable between the camera and the serial port on the back of the laptop. You can connect this just before creating ID cards, so that you are not tied to the laptop when taking photographs. Connect the camera's power cable between the camera and the surge suppressor. The Quick Take Camera comes with three batteries. The camera can use Nickel Cadmium (NiCad) or lithium batteries. The NiCad batteries can be recharged in the supplied charger. Lithium batteries should never be placed in the supplied charger. Do not mix different types of batteries in the camera. Do not use alkaline batteries in either the Quick Take camera or charger.

   b. **Kodak DC220/DC265/DC280:** Connect the camera interface cable between the camera and the serial port on the back of the laptop. You can connect this just before creating ID cards if you like, so you are not tied to the laptop when taking photographs. If running off of AC power, connect the camera's power cable between the camera and the surge suppressor. The Kodak camera comes with four AA Alkaline and four rechargeable batteries and a battery charger. You can use standard 1.5 volt alkaline, rechargeable 1.2-Nickel Metal Hydride (NiMH), or rechargeable 1.2V NiCad batteries. NiMH batteries tend to give the best overall performance of rechargeable batteries. Caution: Other types of batteries should never be placed in the supplied charger. Do not mix different types of batteries in the camera or charger. If not already installed, insert the Kodak Picture Memory Card in the slot on the side of the camera.

5. **Laminator:** Plug the power cable into the surge suppressor.

   Note: The ideal temperature for lamination falls between 250-350 degrees Fahrenheit.

6. **Surge Suppressor:** All power cords from the Deployable system components should be plugged into the surge suppressor and the surge suppressor plugged into a 110 VAC power source (wall power outlet, power generator, power inverter, or power transformer).

7. **PCMCIA Communications Card:** If using optional communications to DEERS, plug the communications card into the top PCMCIA slot, if not already plugged in. The PCMCIA slots are on the side of the laptop. Connect the supplied interface cable to the communications card and the phone line or LAN jack.

8. **PCMCIA MRT Framegrabber Card:** If using an optional fingerprint scanner, plug the MRT PCMCIA Framegrabber card into the bottom PCMCIA slot, if it is not already plugged in. The PCMCIA slots are on the side of the laptop. Connect the supplied cable to the Framegrabber card. The cable for the Framegrabber will have an RCA/BNC connector on the end; always keep it attached so you do not lose it. Caution: This is a delicate connector!

9. **Fingerprint Scanner:** Connect the Framegrabber interface cable to the Video Out port on the back of the fingerprint scanner. This is a screw on connector; slide the connector on part way, align the notch on the end of the cable with the bump on the connector on back of the fingerprint scanner, then turn the connector clockwise as you push it on. (For disassembly you would turn it counter-clockwise as you pull it off). Connect the power cable between the fingerprint scanner's DC 12V port and the surge suppressor. Plug the dongle, which comes with the fingerprint scanner, between the laptop's printer port and the printer's interface cable to ensure the fingerprint capture software will operate.

10. **USB Hub:** If using a bar code scanner, smart card printer, or smart card reader/writer you will need to use the USB hub to connect these hardware devices to the laptop computer.

Connect the supplied cable between the USB port on the back of the laptop to the USB hub's input connector. The output ports can be used to connect additional hardware devices.

10.3.2.3 System Disassembly

To disassemble the hardware associated with the RAPIDS Deployable System, ensure that the system has first been properly shutdown. See *Section 6.18*, *Quitting Windows NT 4.0*, if you need help on properly shutting down Windows NT. Then follow the remaining steps.

1. Turn off the power switch on the surge suppressor and all other hardware components that have one. Turn the Apple camera off by shutting the lens cover. For the Kodak camera, replace the lens cover and power off the camera.

2. Unplug the surge suppressor from the AC power source.

3. Unplug all power cords from the surge suppressor.

4. Disconnect the individual interface cables between each component and the laptop computer, and then remove any power cables that can be removed from its hardware component. When adapters are used, it is best to keep these connected to the cables so they do not get lost.

5. Disconnect the interface cables from the PCMCIA cards, but leave the PCMCIA cards plugged into the laptop.

6. Neatly coil all cables so they will fit back in the soft-sided carrying cases.

7. Remove the toner cartridge from the printer according to the instructions provided in the printer's manual, and store in the nylon bag provided.

8. Remove all batteries from the digital camera so they do not corrode inside the camera. Keep the Kodak Picture Card installed.

9. When the system is completely disassembled, pack all components, cables, and manuals into the provided soft-sided carrying cases for protection, according to the RAPIDS Deployable Packing Instructions.

Note: These steps should also be followed whenever the system needs to be returned for troubleshooting or maintenance purposes.

10.3.3 Deployable Laptop: Features and Connections at a Glance

These illustrations are only meant to help you understand how to use the laptop computer you have as part of deployable RAPIDS, and do not replace the laptop manufacturer's instructions. Deployable RAPIDS currently supports the Panasonic Toughbook CF-27.

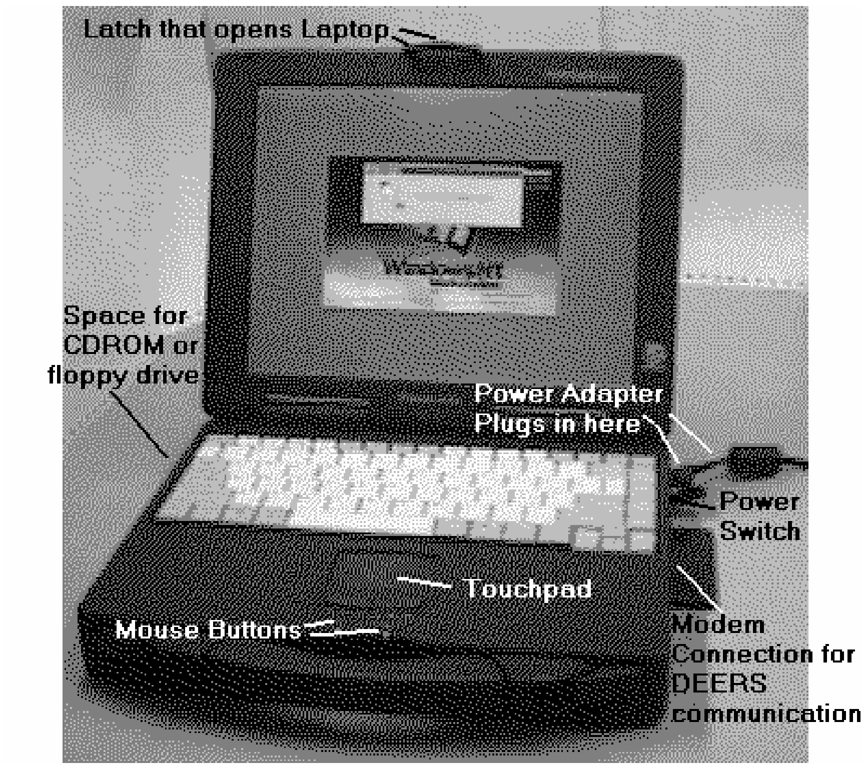
Instead of a mouse, this laptop has a touch pad that, if you sit square to the keyboard facing the display panel, is located between you and the keyboard.

Make note in the following illustrations of the front and back of the laptop where various features and connections are located.

To open and close the Panasonic Laptop use the following procedure.

1. Pull carry handle forward and locate the latch on the front edge of the laptop's cover.
2. Lift up the latch with your finger.
3. Lift open the LCD panel to a comfortable viewing angle.

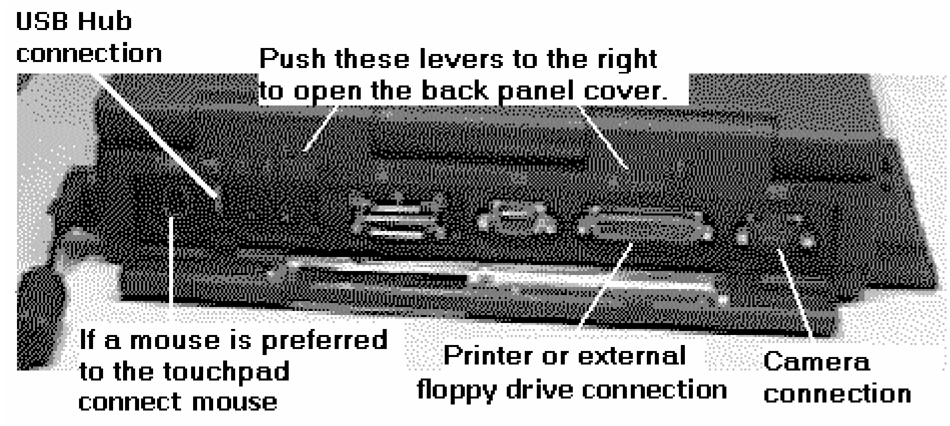
After turning off the laptop, to close the LCD panel, simply lower the panel over the keyboard pressing down until the latch catches to secure the panel.



Panasonic CF-27 Laptop

Changes needed to the above graphic: (1) Remove the word "space" and say "Device Bay". (2) Replace "Modem connection for DEERS Communication" with "PCMCIA slot- PCMCIA cards fit here".

To turn the Panasonic Laptop's power on and off: After opening the laptop, slide the Power lever on the side of the laptop toward the power adapter plug-in (right rear corner on the side) as far as it will go, hold for approximately one second, then release the lever. In a moment, you will see green lights flicker on below the mouse buttons, and the laptop will boot up. To turn the laptop off, first properly shut down Windows NT; your laptop will automatically shut down. Once the laptop has shut down, close the LCD panel.



Back view of Panasonic CF-27 Laptop

Update needed to graphic: (1) remove the word “connect” in the mouse description above and (2) add USB Hub connection.

Panasonic Laptop’s Back Panel Interface Ports: To access the interface ports on the back of the Panasonic laptop, press the levers above the Back Panel Cover and it will drop down to reveal the interface ports. The printer and digital camera connect to the ports as shown in the figure above. For the Panasonic CF-27 laptop only, you can connect a USB Hub to the USB port to provide additional interface ports, which may be used to connect optional hardware devices, such as a bar code scanner, smart card printer, and smart card reader/writer. If you do not want to use the touchpad, you can connect a PS/2 mouse to the back of the laptop as shown above. The keyboard port can be used to attach an external keyboard or PIN keypad.

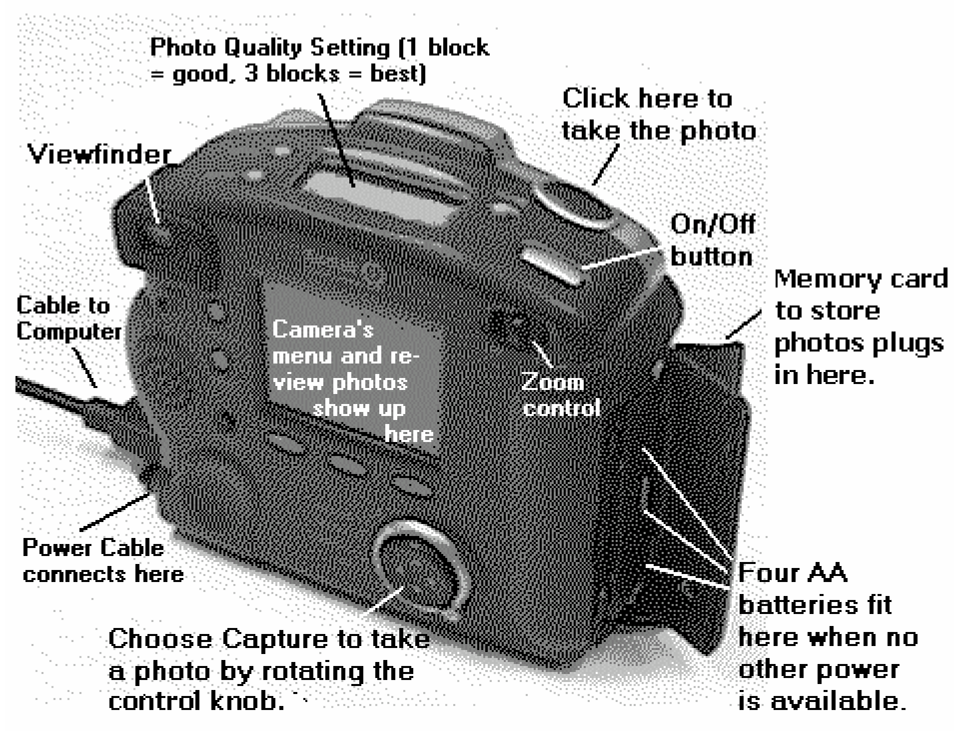
10.3.4 Deployable Camera: Features and Connections at a Glance

These illustrations are only meant to help you understand how to use the camera you have as part of deployable RAPIDS and do not replace the camera manufacturer's instructions. Please follow our recommendation in this Training Guide to learn to use the camera **before** your unit is deployed. Deployable RAPIDS includes one of three cameras, so refer to the appropriate section below for your camera make/model.

Note: For all cameras, always use the highest resolution setting for the picture quality on the digital camera. See the camera’s manual for details on how to select this mode.

To turn the Kodak Camera on and off: Press the Power button on the upper right side of the camera, and then release it. The Ready light blinks green for about six seconds, before the camera is ready. In a moment the lens will extend, and the camera will be ready to take photographs. To turn the camera off, press the Power button and hold it for at least one full second.

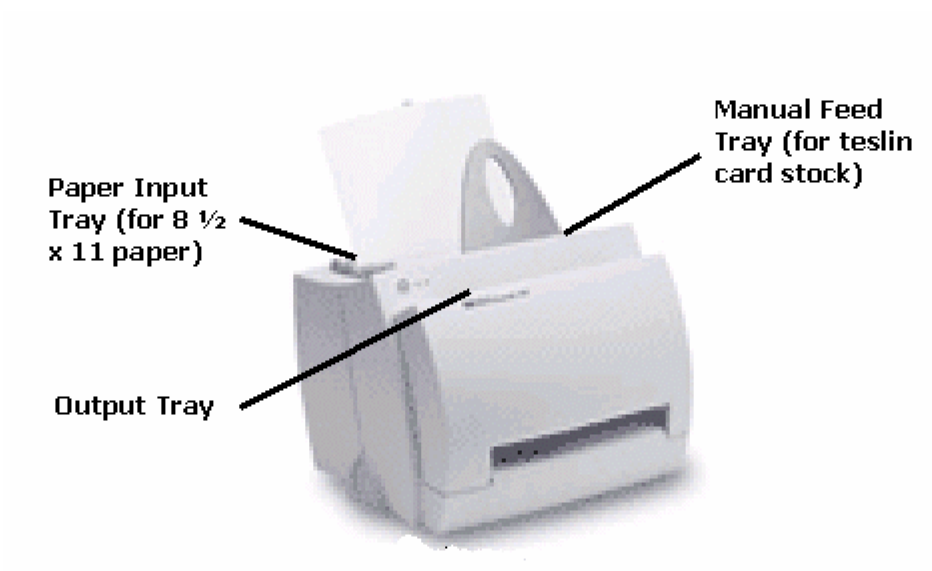
To Take Pictures with the Kodak Camera: The shutter button is located on the top right of the camera, near the front. Pressing the shutter button causes the camera to take a photograph. For more details, see *Section 10.8.*



Kodak DC220/DC265 Zoom Camera

10.3.5 Deployable Laser Printer: Features and Connections at a Glance

These illustrations are meant to help you understand how to use the laser printer you have as part of deployable RAPIDS, and do not replace the printer manufacturer's instructions. Deployable RAPIDS includes one of three laser printers. Refer to the appropriate section for your printer make/model.



Hewlett Packard 5L and 5L-FS Laser Printer

To turn the HP 5L and 5L-FS Laser Printer on and off: The LaserJet 5L/5L-FS printer does not have an On/Off switch, it is **on** whenever it is plugged in. If the printer is inactive for 15 minutes, the printer will automatically enter **Sleep Mode**. When in Sleep Mode, the printer can be awakened by starting a print job through the software, pressing the Front Panel Button, or opening the Printer Door. The printer will retain the present fonts, macros, and printer settings while in Sleep Mode. After waking up, the Ready Light will be green, and the printer will be ready to print ID cards and DD Forms 1172. To turn the printer off, you need to either turn off the surge suppressor's On/Off switch or unplug the laser printer.

To load paper in the HP 5L and 5L-FS Laser Printer: Load 8 ½ x 11 plain white bond paper in the Paper Input Bin, as follows. The Paper Input Bin holds up to 100 sheets of paper.

1. Raise the Paper Input Support located on the top of the printer behind the Paper Input Bin, until a click is heard.

2. Insert up to 100 sheets of paper into the Paper Input Bin. The Ready Light will be lit green if the paper is loaded correctly.

Note: When adding paper to the Paper Input Bin, take out the paper already in the bin. Add the new paper to the pile. Shuffle and straighten into a neat pile before placing the stack in the bin. Do not simply add paper to the pile already in the Paper Input Bin.

Installing a Toner Cartridge in the HP 5L and 5L-FS Laser Printer: To install the toner cartridge or replace a used toner cartridge, follow the instructions in the printer's manual.

Caution: HP recommends NOT using refurbished toner cartridges; only new toner cartridges should be used. See the printer's manual for the proper part number to order.

HP 5L and 5L-FS Front Panel Status Lights and Button: The front panel of the HP LaserJet 5L/5L-FS contains three status lights and one button.

- **Error (top) Light:** Yellow: steady when an error occurs (i.e., out of paper), blinking when the page sent is too complex for the printer (causing a memory error), or off when the printer is in Sleep Mode.
- **Data (middle) Light:** Green: steady when the printer is busy receiving data, blinking when the printer is in Manual Feed Mode, or off when the printer is in Sleep Mode.
- **Ready (bottom) Light:** Green: steady when the printer is ready to print, blinking when the printer is busy receiving data, or off when the printer is in Sleep Mode.

Printing an ID Card Using Manual Feed Mode: The Manual Feed Mode should be used when printing the ID card.

1. Select the printer's Manual Feed Mode according the printer's manual. Set the Paper Path Lever to the lower position for a straight-through paper path. The Manual Feed Mode is selected if the Data Light is blinking.

2. Ensure that the correct cardstock has been placed in the Single Sheet Input Slot (located on the top of the printer, behind the Paper Output Support) in between the two sliding paper guides. The cardstock should be inserted face up with the top pointing down into the opening.

3. Adjust the two sliding paper guides up against the cardstock.

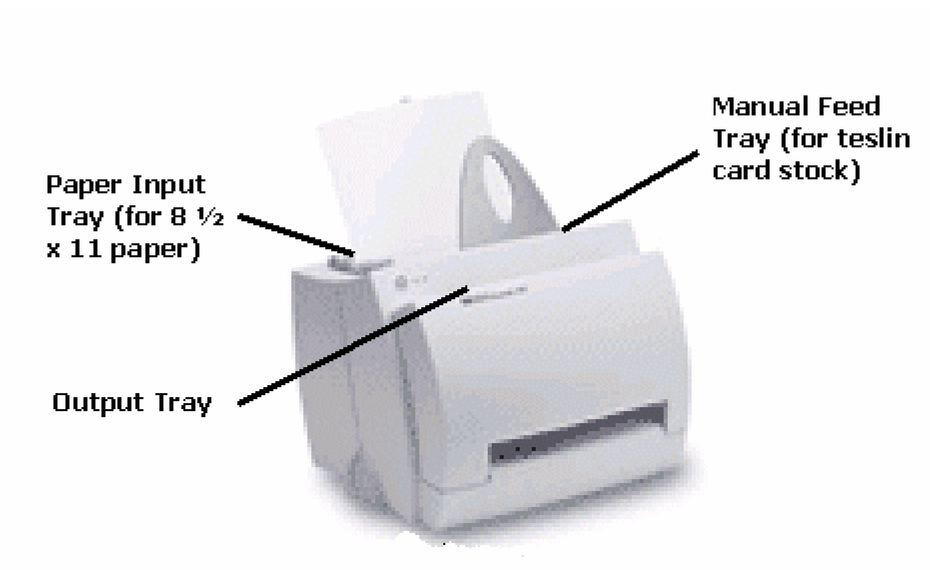
4. Make certain that the card stock is straight.

5. The printer will feed the paper once you select Print ID Card from the RAPIDS application.

6. After the first side is done, turn the cardstock over and insert it into the Single Sheet Input Slot to print the backside of the ID card.

7. Repeat steps 2-5.

Note: Each site is responsible for supplying its own teslin ID card stock for ID card production, 8 ½ x 11 paper for printing DD Forms 1172, and replacement toner cartridges.



Hewlett Packard 1100 Laser Printer

To turn the HP 1100 Laser Printer on and off: Printers that require 110 – 127 volts of power do not have a power switch. Unplug the printer to turn it off. Printers that require 220-240 volts of power have a power switch on the back of the printer.

Loading paper in the HP 1100 Laser Printer: To load plain 8 ½" x 11" paper in the printer, insert the paper in the Paper Input Tray. This is the tray/slot closest to the rear of the printer. Adjust the paper guides as needed.

Loading cardstock in the HP 1100 Laser Printer: To load the teslin cardstock in the printer, insert the cardstock color side facing the front of the printer and upside down in the Manual Feed Tray, one piece at a time. Be sure to adjust the paper guides as needed.

Note: The single sheet paper input tray is the second closest tray/slot toward the rear of the printer.

Installing a Toner Cartridge in the HP 1100 Laser Printer: To install the toner cartridge or replace a used toner cartridge, follow the instructions in the printer's manual.

Caution: HP recommends NOT using refurbished toner cartridges; only new toner cartridges should be used.

HP 1100 Front Panel Status Lights and Control Button: The front panel of the HP LaserJet 1100 contains two status lights and one button with a light.

- **Go Button Light (left):** on when certain errors occur (i.e., out of memory); blinking when the printer is in Manual Feed Mode, during reset, or during initialization; or off when the printer is in Power Save Mode.
- **Ready Light (middle):** on when the printer is ready to print or when fatal errors occur; blinking when the printer is busy receiving data, during reset, or during initialization; or off when the printer is in Power Save Mode.
- **Attention Light (right):** on during printer initialization, reset, and when certain errors occur (i.e., out of paper); blinking when the printer door is open, no toner cartridge, or paper jam; or off when the printer is in Power Save Mode.

Printing an ID Card Using Manual Feed Mode: The Manual Feed Mode will be used when printing the ID card. The Manual Feed Mode is selected when the Go Button light is blinking. It may be necessary to press the blinking green light.

Note: Each site is responsible for supplying its own teslin ID card stock for ID card production, 8 ½" x 11" paper for printing DD Forms 1172, and replacement toner cartridges.

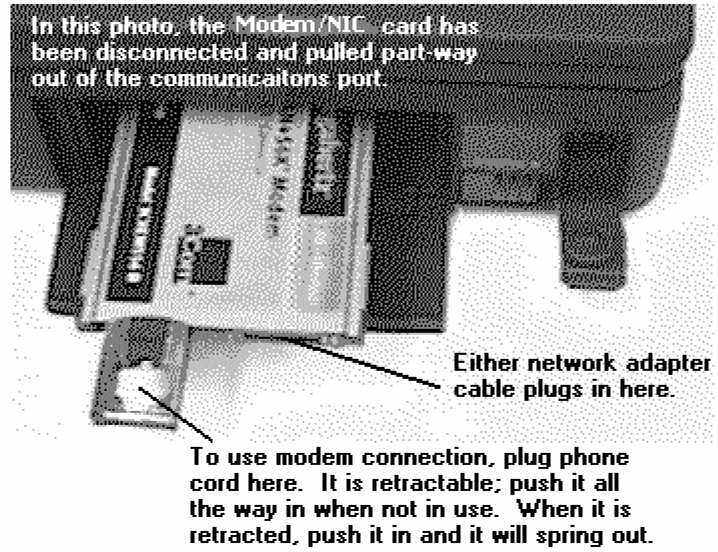
10.3.6 Deployable PCMCIA Communications Cards: Features and Connections at a Glance

In order to make a connection to the DEERS database via a RAPIDS server, you need either a modem and dial-up phone line or a network interface card (NIC) and LAN. Deployable RAPIDS will have one of the following PCMCIA communications cards: PCMCIA modem (3Com/Megahertz, Megahertz, Apex Data, or Smart Modular), PCMCIA Ethernet NIC (3Com), or PCMCIA combination card that contains both a modem and an Ethernet NIC (3Com/Megahertz).

These PCMCIA cards come with adapter cables that are specially designed for use with the particular PCMCIA card. The adapter cables connect the card to the network jack or telephone jack used for communications connectivity.

Each of these PCMCIA cards is designed to slide into the laptop's PCMCIA slot. The *Deployable Laptop: Features & Connections at a Glance* section contains a picture of a Panasonic laptop, showing you where to look for the PCMCIA slots on the laptop. The LAN/modem card fits into the top slot in the laptop.

The illustrations below will help you understand how the PCMCIA communications cards are connected and used. This figure shows the PCMCIA combination modem/Ethernet NIC card, but the others are very similar.



Using PCMCIA Cards in the Deployable Laptop

For instructions on how to make a communications connection with DEERS using the PCMCIA modem and/or Ethernet NIC, see *Section 10.4.3*.

10.3.7 Deployable PCMCIA Framegrabber Card and Fingerprint Scanner: Features and Connections at a Glance

Some RAPIDS Deployable laptops are equipped with a PCMCIA Framegrabber and fingerprint scanner for capturing fingerprints from personnel in an annuitant status during the issuance of the ID cards. The fingerprint scanner is connected to the laptop computer via the PCMCIA Framegrabber card.

Refer to *Section 6* of this Training Guide which details the DEERS/RAPIDS fingerprint capture process and instructs the user on obtaining good quality fingerprints.

To turn the Fingerprint Scanner On and Off: Turn the **Power** switch on the back of the fingerprint scanner to the **On** or **Off** position.

10.4 Configuring and Establishing Communications on Your Deployable RAPIDS System

Three types of communications options are available to support Deployable RAPIDS system connectivity. You must select one of the three connectivity options listed below and identify the Internet Protocol (IP) addresses, firewalls, Ethernet drops, analog phone lines, or login IDs required to establish connectivity for each Deployable RAPIDS system that will be used.

1. LAN connectivity via Ethernet
2. Dial-up connectivity using centralized dial
3. DISN 1-800 Dial-Up Service.

Procedures for the RAPIDS SSM to establish communications using the LAN or dial-up remote access service (RAS) follow.

Please try this at home! It is an excellent idea to try these procedures before your unit deploys, when you have the certainty of communications, and when there is less pressure than you would find trying to establish communications for the first time in a deployed situation.

10.4.1 Logging on to Deployable RAPIDS as Administrator

To log in to deployable RAPIDS as the system administrator, use the following procedures.

1. Close any programs that are running on deployable RAPIDS and restart the computer. You can click **Start**, and then select **Shut Down.** Then select the **Close all programs and log in as different user** option button.
2. Press CTRL+ALT+DELETE to advance to the Authorized Users Only screen. At the end of the text, two codes appear in a single set of parentheses. These are encrypted codes that contain the login ID and password for the administrator account on this computer.
3. Call the D/RAC / D/RSC-E / DSO-A and tell them you need to log in to your deployable RAPIDS as administrator. They will ask you to read the codes at the bottom of the

Authorized Users Only screen. Then, they will tell you the one time password for the administrator account.

4. Click **OK** to advance to the Login Information screen.

5. Type administrator in the User Name text box (or another user name, if a different one was supplied to you by the D/RAC / D/RSC-E / DSO-A).

6. Type the password supplied to you by the D/RAC / D/RSC-E / DSO-A in the corresponding text box, and then click **OK**. You will be logged on with administrator permissions, and you can continue on to step two of the process to establish communications using a NIC.

10.4.2 Initial Installation Procedure: Adding a Machine Name

1. Cable up all network cables if not already done so.

2. Log in with administrative privileges. (See *Section 10.4.1* of this Training Guide.)

3. Right-click on the Network Neighborhood icon and select **Properties**.

4. Add the computer name using the following procedures.

- **Click** Change **from the** *Identification* **tab (if needed).**
- **On the Identification Changes dialog box, type in the computer name from the Site Information sheet.**
- **Click** OK **on the Identification Changes dialog box.**
- **Click** 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."**
- **Restart the machine.** Note: **The computer name and the workgroup name must be added separately as two steps. It is necessary to reboot the machine in between these two steps.**

5. Verify/add the workgroup name. If the workgroup name does not display the name listed on the Site Information sheet, add the workgroup name as follows:

- **Login with administrative privileges.**
- **Right-click the Network Neighborhood icon and select** Properties**.**
- **Select Change from the** *Identification* **tab.**
- **Select the** Workgroup **option button and type in the workgroup from the Site Information sheet.**
- **Click** OK **on the Identification Changes dialog box.**
- **Click** OK **at the message box, "Welcome to the [Domain Name] domain."**
- **Select** Close **within the Network dialog box.**

6. 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?"

10.4.3 Deployable Communications: Configuration for Ethernet/LAN Communications

The following procedure is used to configure TCP/IP when using either Dynamic Server Configuration Protocol (DHCP) or Ethernet.

Note: Disregard this section if the deployable laptop will not be used for LAN based communications.

When you want to establish communications with DEERS using a PCMCIA network interface card (also called Network Adapter or NIC), first log out of all programs including RAPIDS, since a reboot is part of the process of establishing the connection. Before you begin, you need to determine whether the server site uses DHCP or if you will be given a static IP address with which to connect.

If you will be given a static IP address, obtain the subnet mask and default gateway address from your local communications group. All three are numeric codes that contain dots between four sets of numbers (e.g., 123.123.123.123). Know the correct dot placement before you enter the codes in their respective text boxes, as part of the following procedure.

Note: The RAPIDS SSM in conjunction with the local communications group is responsible for determining whether a firewall will be traversed when using Ethernet/LAN connectivity. If so, it is absolutely critical that all appropriate firewall ports are open. These firewall ports are port 3002 for pull/push of data and port 4009 for Oracle database synchronization.

The following procedure is used to configure TCP/IP when using either DHCP or Ethernet. Disregard these procedures if the Deployable laptop will be used for dial-up communications only.

1. Cable up all network cables.
2. Login with Administrative privileges (See *Section 10.4.1* of this Training Guide).

- **Right-click the Network Neighborhood icon and select** Properties.

3. Verify/add network adapters.

- **Click the** *Adapters* **tab from the Network dialog box.**
- **If the 3COM Mhz LAN+56K Modem PC Card (Ethernet) adapter already displays, go to step five. If not, click** Add **on the** *Adapters* **tab.**
- **Click** Have Disk **on the Select Network Adapter dialog box.**

4. If this will be set up as a DHCP Ethernet Workstation, then use the following procedure.

- **Right-click Network Neighborhood, and select Protocols.**
- **Select "Obtain an IP address from a DHCP server."**
- **Proceed to step ten.**

Note: A properly configured DHCP server must exist on the same network as the DHCP workstation, in order for a DHCP Ethernet workstation to function properly.

5. Click the ***Protocols*** tab on the Network dialog box.

6. If the TCP/IP Protocol already displays, go to step seven. Otherwise, select the **TCP/IP Protocol** entry in the Network Protocols list box.

7. Click **Properties** to display the Microsoft TCP/IP Properties dialog box.

- *IP Address* **tab: (repeat for each installed adapter).**
    - ❑ Ensure that the appropriate adapter is selected in the combo box. The card fielded for Guard/Reserve Deployables is **3COM MHz LAN+56K Modem PC Card (Ethernet)**. You will need to validate settings for each adapter that appears in the combo box.
    - ❑ Click the **Specify an IP Address** option button.
    - ❑ Type in the IP address from the Site Information sheet.
    - ❑ Type in the Subnet Mask from the Site Information sheet.
    - ❑ Type in the default Gateway IP address from the Site Information sheet.
- **WINS Address tab:**
    - ❑ Delete IP address 192.147.35.183 for the Primary WINS Server.
    - ❑ Select the **Enable LMHOSTS Lookup** check box.

8. Click **OK** to close the Microsoft TCP/IP Properties dialog box. If a warning message states that the Internet hostname is different than the current computer name or that at least one adapter card has an empty primary WINS address, click **OK** or **Yes** in answer to the warning message, "Do you want to continue?"

9. Click **Close** on the Network dialog box.

   Note: After selecting, the system may take you back to step eight.

10. Click **Yes** in answer to the message, "You must shut down and restart your computer before the new settings will take effect. Do you want to restart your computer now?"

10.4.4 Installing RAS

The following procedure is used to configure RAS when using your modem for dial-up connectivity. This section should be used when configuring your laptop to dial into TSACS or centralized dial devices. Disregard this section if the deployable laptop will not be used for dial-up connectivity.

Note: The RAPIDS SSM, in conjunction with the local communications group, determines whether a firewall will be traversed when using dial-up connectivity using TSACS or centralized dial. If so, it is absolutely critical that all appropriate firewall ports are open. These firewall ports are port 3002 for pull/push of data and port 4009 for Oracle database synchronization.

Deployable RAPIDS systems can connect to DEERS via a military installation's centralized dial device. You do not need to connect to a RAPIDS server, because DEERS will recognize the Deployable RAPIDS system 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 the owner of the centralized dial device. The installation's communications activity can provide this to you.

1. Log in with administrative privileges. (See *Section 10.4.1* of this Training Guide).

2. Install the PCMCIA modem. (If the modem is already installed, skip to step three.):

- **Click Start, and then select Settings|Control Panel.**
- **Double-click the Modems icon and select** Add**.**
- **At the Install New Modem dialog box, select** Don't detect my modem. **Select** Next **to continue.**
- **Deployable Laptops using LAN+56K Modem(3CXEM556B): On the Install New Modem dialog box, select** Have Disk… **. Select** Browse **to the following path:** c:\Archive\Drivers\NICs\Ethernet\3CXEM55x\Disk1\Mdmem556.inf **on the Insert Disk dialog box and select** OK**. On the Install New Modem dialog box, select** 3Com megahertz LAN + 56K Modem PC Card (B) (Modem Interface)**. Select** Next**.**
- **In the Selected Ports list box, highlight the** COM2 **port in the field stating, "You have selected the following modem."**
- **Select** Next **to continue.**
- **If the Location Information dialog box appears, select the appropriate country and area code, and select** Next **to continue.**
- **Select** Finish **to display the Modems Properties dialog box.**

3. Configure the PCMCIA modem:

- **On the Modems Properties dialog box, highlight the device (modem) that needs to be configured, and click** Properties**.**
- **On the** *General* **tab, select the appropriate Maximum Speed of** 57,600 **for PCMCIA Modems.**
- **If the device is a modem, click** Advanced **on the** *Connection* **tab. On the Advanced Connection Settings dialog box, type** &W **for Extra settings. Click** OK **to close the Advanced Connection Settings dialog box.**

- **Select** OK **on the <modem model> Properties dialog box.**
- **Select** No **to the message "Do Dial-Up networking now."** Note: **You will be directed to configure dial–up networking later.**
- **Once the modem has been configured, click** Close **to close the Modem Properties dialog box.**

4. Configure the port used by the PCMCIA modem.

- **Double-click the Ports icon.**
- **On the Ports dialog box, highlight the** COM2 **port from the Ports list box and select** Settings**.**
- **Select the appropriate Baud Rate of** 57,600 **for the PCMCIA Modem.**

  Note: Select the ***Advanced*** tab to configure COM ports three and four if necessary for Smart card machines.

- **Select** Hardware **for Flow Control.**
- **Click** OK **on the Settings for COM*:* dialog box.**
- **Once all of the ports have been configured, click** Close **to close the Ports dialog box.**
- **Close the Control Panel window.**

5. Use the following procedure to install RAS.

- **Right-click the Network Neighborhood icon and select** Properties**.**
- **Select the** *Services* **tab from the Network dialog box.**

  Note: Check to see if RAS is already installed. If not, continue with the following steps to add.

- **Select** Add **from the** *Services* **tab.**
- **Select** Remote Access Service **on the Select Network Service dialog box and click** OK**.**
- **Type in** c:\Archive\WindowsNT **on the Windows NT Setup dialog box and click** Continue**.**
  - Select one of the RAS capable devices on the Add RAS Device dialog box and click **OK**. For example: **3Com megahertz LAN + 56K Modem PC Card (B) (Modem Interface)**.
- **On the Remote Access Setup dialog box, add the remaining RAS capable devices if necessary.**
- **Click** Network **to display the Network Configuration dialog box.**
- **Ensure that TCP/IP is selected and click OK.**
- **Click** Configure **(right of the TCP/IP check box) to configure the Configure Port Usage dialog. Ensure that the dial out only option is selected.**
- **Select** OK **to dismiss the Configure Port Usage dialog.**
- **Click** Continue **to close the Remote Access Setup dialog box.**
- **Click** OK **at the message, "Remote Access Service has been successfully installed."**
- **Click** Close **to exit the Network dialog box.**
- **Select** Yes **to the question, "You must shutdown and restart your computer before the new settings will take effect. Do you want to restart your computer now?"**

10.4.5 Deployable Communications: Creating Dial-up Phonebook Entry

You can establish a dial-up connection with a modem 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, proceed with step one, below.

In order to succeed, you will need to know the telephone number of the modem at the centralized dial / TSACS or 1(800) DISA dial-up service location. You will need a user account for a centralized dial device that accepts incoming calls.

1. If you are attempting a dial-up connection on deployable RAPIDS and no phonebook entry exists for the system you are trying to dial, you must create the phonebook entry. This phonebook entry could be used to connect to the centralized dial device, TSACS, and/or DISN dial up service. If you have any questions regarding this matter, please contact your D/RAC / D/RSC-E / DSO-A. Login with administrative privileges (See *Section 10.4.1* of this Training Guide.)
2. Click **Start** in the Windows NT desktop, then select **Programs|Accessories|Dial Up Networking**. The Dial-Up Networking screen appears.
3. Click **New…**. The first screen of the New Phonebook Entry Wizard appears.
4. In the **Name…** text box, type a name (e.g., dial-up to centralized dial) for the entry you are about to add; then click **Next**.
5. At the Server screen, select **I am calling the Internet** and **Next**.
6. Type the numbers you would have to dial on a telephone from your current location to contact the centralized dial/TSACS server. If you need to dial **9** to get an outside line, you must include it here. If it is a long distance or international call, include **1** followed by the area/country code, prior to the number. Use a comma (,) to indicate a pause (e.g., to wait for dial tone after dialing number(s) to get an outside line).
7. Click **Next;** then click **Finish**. The phonebook entry has been created and is ready for use.

To dial using your modem, continue with the following steps.

1. Login with administrative privileges. (See *Section 10.4.1* of this Training Guide.)

2. In the Windows NT desktop, click Start, then select **Programs|Accessories|Dial Up Networking**. The Dial-Up Networking screen appears.

3. Ensure that the name in the "Phonebook entry to dial" box is that of the server site you wish to dial. If it is not, click on the right side of the box, and then choose the correct entry from the list.

4. When you make your choice, the values in the "Phone Number Preview" and "Dialing From…" boxes will be updated to contain the information that corresponds to the entry you have chosen.

5. Click **Dial**. The **Connect to…** window opens. Type the User name, Password and Domain that have been provided to you by the service site.

6. Click **OK**. You will hear the modem try to connect. If you are successful, the window will close, and an icon in the lower right corner of the Windows NT desktop tells you that you are connected.

7. Double-click  to start RAPIDS.

8. RAPIDS will come online. If it does not, double-click the word "Deployed" in the status bar, and then click Yes to indicate that you want to establish the connection.

10.4.6 Initial Configuration of Database, Devices, and Security

Note: The following steps detail the initial configuration of your deployable RAPIDS system. It is not necessary to follow the steps each time the deployable RAPIDS system is accessed unless the configuration has changed.

1. Log in with administrative privileges.
2. Ensure that the machine can participate in the domain. (Establish a connection to DEERS.)
3. Double-click the RAPIDS Configuration icon on the desktop. The RAPIDS Configuration dialog box will be displayed.

- System **tab:**
    - Click **Machine is a dedicated RAPIDS system** check box.
    - Click **Date and Time**. Use the Date/Time Properties dialog box ***Date & Time*** tab to set the date, time, and the ***Time Zone*** tab to set the time zone. Click **OK** when done with the Date/Time Properties dialog box.
- **Authentication tab:**

    Note: Delete the contents of the Name edit box and fill the IP Address edit box with all zeros.

    - Click **Test** under Administration Service to test the administration services. The response is a dialog box stating you "pinged successfully."
- **Databases tab:**
    - In the Alias combo box, key in the name of the server containing the Oracle database used by this machine.
    - The Primary Name or IP edit box should be faded.
    - In the Secondary Name or IP edit box, enter a secondary IP address only if a static one is provided. If not, leave this field blank.
    - Click **Update TNSNames** to update the c:\orant\network\admin\tnsnames.ora file.
    - Click **Yes** to continue when presented with a RAPIDS Configuration dialog box that contains the message, "This will overlay the TNSNames.ora file with a RAPIDS specific version. Continue?"
    - When presented with a RAPIDS Configuration dialog box that contains the message, "TNSNames.ora file successfully updated," click **OK** to return to the main RAPIDS Configuration dialog box.
    - Start the database and update the listener file using the following procedure.
    - Click **Update Listener** to update the c:\orant\network\admin\listener.ora file.
    - When presented with a RAPIDS Configuration dialog box that contains the message, "This will overlay the Listener.ora file with a RAPIDS specific version. The Oracle database will be disabled while this file is updated. Continue?" click

Yes to continue. This command will take approximately one minute during which time a progress bar will be displayed.

- When presented with a RAPIDS Configuration dialog box that contains the message, "Listener.ora file successfully updated," click **OK** to return to the main RAPIDS Configuration dialog box.
- Click **Test Connection** in the RAPIDS server group on the RAPIDS Configuration dialog box to test the network connection to the database on the RAPIDS server. A progress bar will be displayed briefly stating, "Attempting connection to [database name]." When a connection has been established, click **OK** to return to the main RAPIDS Configuration dialog box.
- Ensure that your communications is active, and click **Test Connection** in the DEERS database group on the RAPIDS Configuration dialog box to test the network connection to the DEERS database. A DOS screen will display with the replies.
- Press any key to return to the main RAPIDS Configuration dialog box.

- **Bar Code Reader tab:**
  - If a bar code scanner is attached to the machine, select the appropriate scanner model from the Bar Code Reader combo box.
  - Select the COM port to which the bar code reader is attached.
- Camera **tab:**
  - If a camera is attached to the machine, select the appropriate camera model from the Camera combo box.
  - Select the COM port to which the camera is attached (**COM1**).
  - If installing a Kodak DC220 or Kodak DC265 Digital Camera, use the following procedure to modify the Port baud setting to **115200** and decrease connection times to the camera.
    - Click **Start;** then select **Settings|Control Panel**. Double-click the Ports icon. Select the port that the to which the Kodak is connected (**COM1**), and click **Settings**. On the Settings for Com dialog box, change the Baud Rate to **115200**.
    - The camera should keep the following default settings for use with RAPIDS. Please feel free to change the format of the items below.
    - Picture Type: Still
    - Flash: Auto
    - Quality: Best
    - Kodak DC220 Digital Camera Resolution: High (1152 x 864)
    - Kodak DC265 Digital Camera Resolution: High (1536 x 1024)
    - White Balance: Auto
    - Watermark: **None**
    - Advanced Exposure Modes: Programmed AE
    - Capture Settings
      - File Type: JPG

- ♦ Quick View: 3 sec.
- ♦ Auto Rotate: On
- ♦ System Sounds: On
- ♦ Sleep Timeout: 2 min.

❑ Camera Name Settings

- ♦ Kodak DC220 Digital Camera: **DC220**
- ♦ Kodak DC265 Digital Camera: **DC265**

Note: The values in **bold** are required values for RAPIDS. The other values are simply recommended.

- **Fingerprint Reader tab:**

❑ If a fingerprint reader is attached to the machine, select the appropriate fingerprint reader model from the Fingerprint Reader combo box (**Identicator DFR-90DF**).

❑ MRT Configuration:

1. Select the fingerprint reader model and Framegrabber types from the appropriate combo box. When Framegrabber type is MRT VideoPort Pro, the Framegrabber Properties section is enabled.

2. If necessary, select any one of the filters:

   - **Smoothness Filter:** A milder averaging filter (**This is the default and is highly recommended**).
   - **Detail Filter:** Enhances detail in the image.
   - **Sharpen Filter:** Sharpens the edges in the image.
   - **AI Sharpen Filter:** AI stands for "anti-interlace." This removes interlace-effects caused by time-delays in full motion video. AI Sharpen combines an AI filter with the Sharpen filter to bring back crispness after removing interlace-effects.

3. If necessary, enter in a new brightness and contrast value. These values affect the brightness and contrast of the grabbed image. The default values are Brightness: **-5** and Contrast: **10**. The valid brightness and contrast ranges are as follows:

	Min Value	**Max Value**
Brightness	-128	127
Contrast	-128	127

- **Printers tab:**

❑ Install printer drivers using the following procedure.

- ♦ Click **Add Printer to System**.
- ♦ Click the **My Computer** option button on the Add Printer Wizard dialog box and click **Next** to continue.
- ♦ Select the port to which the printer is attached (LPT1) in the Available Ports list control and click **Next** to continue.

- Select the appropriate manufacturer and printer.

  Reminder: The Brother HL 960 uses the HP LJ 4 printer driver. If not in the list (HP1100 is not on the list), select **Have Disk**, and enter the following path to install the printer driver: **c:\Archive\Drivers\Printers\HP_LJ_1100**. Click **Next** to continue.

- Click the **Not shared** option button, and click **Next** to continue.
- Click the **Yes** option button, and click **Finish**.
- If the Files Needed dialog box appears, for Copy files from, type in **c:\Archive\WindowsNT**.
- A message box should appear asking if you would like to print a test page. Ensure that the printer is attached and powered on. Click **Yes,** then click **OK**.
- A test page should be printed.
- When the RAPIDS Configuration dialog box is displayed, select the newly installed printer as the RAPIDS ID card and/or smart card printer.
- Suggested offset values for ID cards and 1172 are as follows:
  - ID Card Offsets: front top 2200, back top 2200, Front left: 3390, back left: 3350
  - 1172 Offsets: top: 710, left: 125.
- These will allow the ID card to print within the limits of the actual card and not over the perforated lines. Use the suggestion that best works for your particular site.
- To add a CAC compatible printer, repeat the above process to add the printer.

- <u>If your system has an Internal or External encoder,</u> select the COM port to which the encoder is attached.
- <u>If your system has no encoder,</u> select **None** as the COM port.
- <u>If your system has an S2 Smart card printer w/ in-line encoder,</u> select the In-line encoder check box.
- <u>On other Smart card printers,</u> deselect the In-line encoder check box.

Note: When a smart card printer is installed, make sure that the ID card and DD Form 1172 printer is set as the default.

- *Security* **tab: A progress bar will be displayed briefly.**
  - Click **Activate Site** to add a site to the RAPIDS server. Each Deployable RAPIDS laptop has a unique site ID.
  - Key in the following on the Activate Site dialog box, and then click **OK**:
    - **Site ID:** (from the Site Information sheet)
    - **UIC:** (from the RAPIDS SSM)
    - **Phone #:** (from the RAPIDS SSM)
  - When presented with a RAPIDS Configuration dialog box that contains the message, “Site <#> was successfully added to the transaction database,” click **OK** to return to the main RAPIDS Configuration dialog box.

- Repeat the previous two commands to add the remaining sites assigned to the RAPIDS server. For back-up training purposes, it is advisable for the FSR to also add the EDS/DEERS site ID **101152**.
- Select the Refresh list of available RAPIDS SSMs button.
- Click **OK** to acknowledge the warning on the RAPIDS Configuration dialog box.
- A progress bar will be displayed while the list of RAPIDS SSMs is being refreshed.
- You will return to the main RAPIDS Configuration dialog box.
- Click **Activate SSM** to add an RAPIDS SSM for a given site.
- Click **SSM** on the Activate SSM dialog box and then click **OK**.
- Repeat the previous two commands to add the remaining RAPIDS SSMs for the sites assigned to the RAPIDS server.

4. Click **Close** to close the RAPIDS Configuration dialog box. A progress bar will be displayed briefly.

5. Double-click the RAPIDS Configuration icon on the desktop again. Select the ***Authentication*** tab and ensure for all systems <u>except</u> deployable that the information under Authentication Machine is complete. **A known bug is that it may be necessary to delete the Name and IP address entries a second time**. If not, return to the ***Authentication*** tab instructions at the beginning of this document. Click **OK** to close the RAPIDS Configuration dialog box. It is possible that you may see several <u>expected</u> warning messages stating that X parameters were not initialized. Click **OK** after each message.

10.4.7 Apply Windows NT Post-Release Software and Create Emergency Repair Disk

1. Log in with administrative privileges (you may already be logged on from the previous procedure).

2. Select **Start** and select **Run**.

- **Run the following command:** d:\setup.bat**. You will see an MS-DOS window open stating that it is not necessary to be connected to DEERS to perform an update.**

3. Create an Emergency Repair Disk.

- **Put a blank 3.5” HD floppy disk in the a: drive. (Do not use the original repair disk, if one exists).**
- **Click** Start **and select** Run**.**
- **Run the command** rdisk**.**
- **Click** Update Repair Info **on the Repair Disk Utility dialog box.**
- **Click** Yes **if prompted with, “The repair information that was saved when you installed the system or when you last ran this utility will be deleted. Do you want to continue this operation?” A Saving Configuration progress bar will appear.**
- **Click** Yes **at the message box, “Do you want to create the Emergency Repair disk?”**

- **Click** OK **at the message box, "Warning: All data in the floppy disk will be erased." A Formatting Disk progress bar will appear and will be followed by a Copying Configuration Files progress bar.**
- **Click** OK **at the message box, "Windows NT repair information contains security sensitive data. Please ensure that the emergency repair disk you just created is stored in a safe place accessible only to administrators of this system."**
- **Click** Exit **to close the Repair Disk Utility dialog box.**
- **Remove the 3.5" floppy disk and label it as follows: NT 4.0 Deployable Emergency Repair Disk. <PC NAME> <DATE> <TIME>.**

10.4.8 Installation Testing/Validation

1. The RAPIDS SSM activated in the previous steps should complete the following procedure.

- **Log in using the initial password BASEBALL, and start RAPIDS.**
- **Select** Tools|User Administration **from the menu bar. The RAPIDS User Security Navigator dialog box appears.**
- **Click the** Update User **option button.**
- **Click** Next**. A progress monitor will briefly display.**
- **Select the name on the RAPIDS User Security Navigator – Update User dialog box.**
- **Click** Next**. A progress monitor will briefly display.**
- **Acknowledge any error messages that appear regarding the password.**
- **Click** Next **on the RAPIDS User Security Navigator – DEERS Security dialog box.**
- **Add the VO, IO, and SVO roles.**
- **Click the** Update Password **check box and type in the user's DEERS password twice. (This would be the password that arrived within the secure gray envelope. If necessary, this password can be reset through the D/RAC / D/RSC-E / DSO-A).**
- **Click** Finish **on the RAPIDS User Security Navigator – RAPIDS Security dialog box.**
- **Click** Yes **or** No **at the question, "Do you wish to perform another security function?" This is an opportune time for the RAPIDS SSM to add and assign roles to the remainder of the RAPIDS users for this site.**
- **If** No **is selected, exit RAPIDS.**

2. Start RAPIDS, open a family, and create a DD Form 1172 and ID card.
3. Shut down RAPIDS, and restart the machine.

10.5 Deployable 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 system. The subsections under this heading discuss three aspects of user administration that are particular to deployable RAPIDS.

10.5.1 Deployable RAPIDS and the SSM User Role

When any user account is created on deployable RAPIDS, the RAPIDS SSM role is automatically granted to that user. This means that, by default, all deployable RAPIDS users can add, modify, and delete user accounts, and perform any of the other RAPIDS SSM functions while operating the system in deployed mode (that is, without communications). The generic user account is also assigned the SSM user role (see Section 10.5.3).

10.5.2 Creating and Registering User IDs on Deployable RAPIDS

For communications and security purposes, each deployable RAPIDS is regarded as a "RAPIDS site." In order for the records sent by a deployable RAPIDS user to be accepted by DEERS, the sending user's ID must meet the following criteria.

- The ID must be created on that deployable 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,.
- The ID must be registered for use at the RAPIDS site corresponding to the deployable RAPIDS system they will use.

There are two ways to set up an account on deployable RAPIDS.

1. **Create and register DEERS user IDs in online mode ahead of time.** This is the preferred method because you can create and register the user IDs when communication is 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* of this Training Guide). The user ID is, in this case, registered automatically.

   Therefore, when RAPIDS users who will have to use deployable RAPIDS are identified a few days before the deployment, connect the deployable unit 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 is what may be necessary if you must 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 mode requires some form of verbal or message communication with the DEERS/RAPIDS Security Office or the D/RAC / D/RSC-E / DSO-A. If phone lines, e-mail, or some other communication is not available, it is not possible to use this method. Call the DEERS/RAPIDS Security Office at 1-800-3RAPIDS, extension 5006 or 5007, send an e-mail (call and ask for the e-mail address), or send regular mail to 1600 N. Beauregard Street, Attention: Security, Alexandria, VA 22311. Tell them why you are calling, and provide the following information.

- **The site ID of the deployable RAPIDS laptop for which the user needs to be registered on your deployable workstation. (This appears in the first screen of the RAPIDS User Security Navigator.) Then select** Tools|User Administration **from the RAPIDS menu bar to view it.**
- **Provide the name of the person who will need to use the deployable RAPIDS.**

This process requires 24 hours to complete. The following business day, the DEERS/RAPIDS Security Office can provide to the site two character strings, which should be typed into the Encrypted Data and Decryption Key text boxes when prompted by the RAPIDS User Security Navigator.

Add the user account as you would normally add any user account, referring to the instructions in *Section 9.2.2*, *Add New User*, in this Training Guide. At the beginning of the navigator, an extra screen appears, prompting you to enter the Encrypted Data and Decryption Key. Fill in these fields with the character strings that were provided to you by the Security Office.

10.5.3 Generic User ID on Deployable RAPIDS

Each Deployable RAPIDS system is configured with a generic user account. This allows your unit to continue issuing ID cards and to perform other RAPIDS actions in extreme situations in the event that no person who has a 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 they create can be sent to DEERS by a user whose ID has been registered.

Every unit that may use deployable RAPIDS should ensure that all personnel who use deployable RAPIDS know the generic user ID and password so that they can issue ID cards during the deployment.

10.5.4 Deployable Theft Protection and the Key Master

RAPIDS deployable systems run a much higher risk of theft than desktop systems. It is expected that desktop systems are used in secured areas, whereas deployable units are frequently used in public spaces. Because of this increased risk and because deployable systems are designed to operate for extended periods without communicating with DEERS security services, the deployable systems need 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 systems, 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 unlock key. A locked system will not allow the use of RAPIDS. Users will still be able to log in to Windows NT, but they will be told that the use of RAPIDS has been suspended. If a user tries to run the RAPIDS application while the system is locked, they will receive the message box, "The security system of this dedicated RAPIDS machine has been compromised. Please contact the RAPIDS

Assistance Center for more details. RAPIDS will now exit." The *Key Master* and an NT 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 ID cards. Of course, to create ID cards on a stolen system, the thief would also need to have stolen user credentials and cardstock. If the thief has stolen the *Key Master* password, then the need to reset the system after the number of unlocks has been exceeded should minimize the amount of time that a stolen system could be used to create ID cards. The system must be reset after the specified number of unlocks (default is ten) has been exceeded. A Windows NT administrator is the only one that can reset the system.

When a user logs on to a RAPIDS deployable system, the watchdog application checks the following before authorizing use of RAPIDS.

Key Master password. If the 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." The following text is placed in the Windows NT application event log: "The login monitor has determined that the Key Master password has been tampered with. Use of RAPIDS is being 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 following text is placed in the Windows NT application event log: "The use of RAPIDS on this system has been suspended, and the maximum number of Key Master unlocks 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 the correct password is given, the following text is placed in the Windows NT application event log: "The system has been unlocked by the Key Master. This is the X of Y available unlocks." 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." The following text is placed in the Windows NT application event log: "An unsuccessful attempt was made to unlock the system using the Key Master password. Use of RAPIDS is still suspended." After acknowledging the message box, the user is unable to use RAPIDS.

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 an NT 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.

10.6 Logging on to Deployable RAPIDS

1. If the computer is turned off, ensure that any peripherals are properly connected to the computer and turned on, before turning on the computer.

2. Turn the laptop computer's power on and let the machine boot up, if necessary. You are ready to proceed when the Begin Login screen appears.

3. Press CTRL+ALT+DELETE, and then press ENTER to close the security information message. The Login Information screen will appear.

4. Type your DEERS/RAPIDS user ID and password (in capital letters) into the corresponding text boxes, and then press ENTER. In a moment, the Windows NT desktop will appear.

5. Double-click the RAPIDS icon on the desktop. The RAPIDS main screen will open in the background, with the Message of the Day window active in the foreground.

   Note: The Message of the Day may not be updated if communication is not established regularly.

6. After you are finished reading the Message of the Day and RAPIDS Tip, click **Close** in the bottom right-hand corner of the Message of the Day window. You are now ready for RAPIDS data processing.

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, printing the DD Form 1172, and creating the cards. This is covered in detail within *Sections 5 through 7* of this Training Guide.

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 Active Duty ID cards, Guard/Reserve ID cards, and Civilian Geneva Conventions ID cards. The process of ID card creation on deployable RAPIDS is similar to that of creating an ID card on standalone RAPIDS.

The differences involve the camera and ID photograph. Whether you have the Apple or Kodak camera, the following strategy will greatly speed up the production of ID cards. Take a batch of pictures while the camera is disconnected from the system. Note the photo number for each individual photograph. When you have taken all the pictures, connect the camera to the laptop, boot up the laptop, and use RAPIDS to create all the ID cards at one sitting. The value of this strategy increases with the number of cards you need to produce and will save you significant time even if you only need to produce two ID cards.

An alternate method is to capture the photos one at a time and download them separately in the ID card Navigator.

The  Create Card Navigator allows the user to create an ID card. Once the family has been saved to DEERS, the user can create the ID card. The Create Card Navigator is detailed in Section 6.4.1 of this Training Guide.

10.6.1 Creating ID Cards Using the Kodak Deployable Cameras

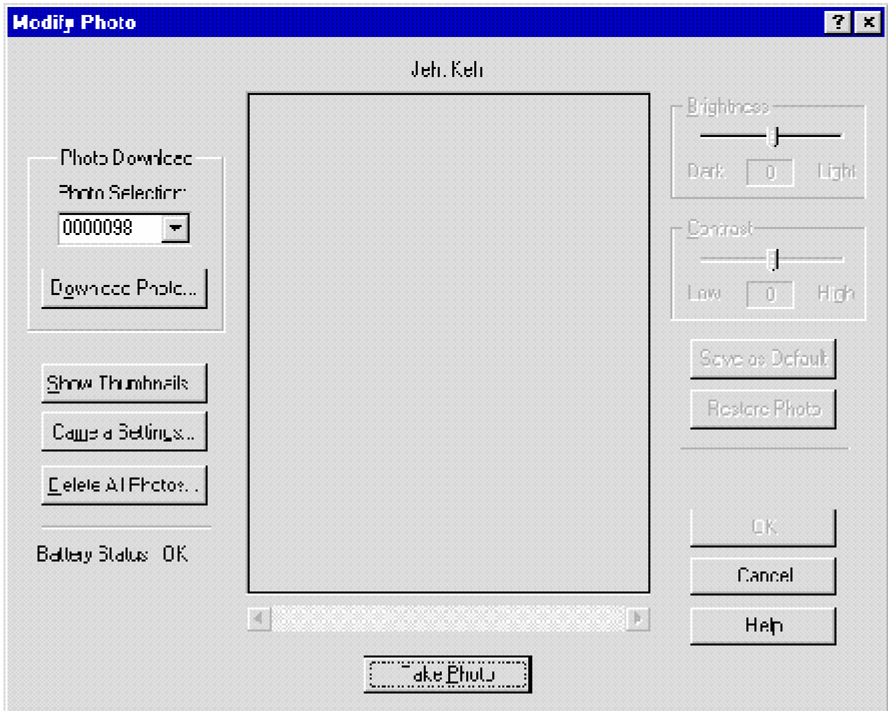
The following steps should be used to create ID cards with the Kodak deployable camera.

1. After having identified the persons for whom ID cards must be created, take all the photographs without connecting the camera to the laptop computer. The round control knob near the bottom of the back of the camera must be set to **Capture** (the top setting).
   a. The memory card, a square, flat card that stores the photographs in the camera, fits inside a slot on the side of camera and must be installed with space available for more photographs.
   b. Notice that after you take each photograph, it will appear in the large display window on the back side of the camera and remain there for a few seconds with its photograph number. Make a list of names with photograph numbers as you take the photographs.
   c. You can review all the photographs and their numbers on the camera by setting the control knob to Review (second setting from the top) and then pressing the left and right arrow keys on the control knob to scroll back and forth, one photograph at a time.

2. When all the photographs have been taken, set the control knob in the back of the camera to Connect (third setting from the top), and connect the camera to the computer, using the cable provided for this purpose.

3. In RAPIDS, open or create the family record for one of the persons whose photograph you have taken. Use the Create ID Card Navigator (see *Section 10.6.1* in this Training Guide).

4. When you reach the Modify Photo dialog box, in the Photo Download section on the left side of the dialog box, use to select the correct photograph number from the choice list. Below is a screen print of the Modify Photo dialog box.



5. Click **Download Photo**. A progress monitor will show you the progress of the download from the camera. When finished, the image appears in the Modify Photo window.

6. You may use the Brightness and Contrast controls on the right side of the window to fine tune the image by clicking and dragging the indicator arrows to the left or to the right.

7. Click **OK** to advance to the next navigator screen. The Create ID Card navigator will walk the end user step-by-step through the printing of the ID card.

8. Repeat steps 3-7 above for each person with photographs saved on the camera's memory card. After all ID cards have been created, delete the photographs from the memory card using the following procedure. Turn the mode dial to the Review setting. It may be necessary to press **Display** if no display shows. To delete a single picture, press DELETE. You will be prompted to confirm the delete, and then press DELETE again. To delete all photos, press DELETE for two seconds. A confirmation screen appears asking if you want to delete all the pictures on memory card. Press Delete All.

10.6.2 Kodak Camera Settings

The Kodak deployable camera allows you some extra image quality settings. You should only attempt to change these settings if the image quality is consistently poor. To access these options, click Camera Settings on the left side of the Modify Photo window, while the camera is connected to the laptop computer. Select the setting for best picture quality, High resolution, Auto flash, and Auto white balance.

- **Best Picture Quality** and **High Resolution** afford the best image quality but reduce the number of pictures that can be stored on the camera's memory card.

- **Flash Mode Auto** will cause the flash to fire when the camera senses there is not enough light without the flash. Choose Red-eye Reduction if this is a problem, but if this camera is used often in battery mode, you should be aware that repeated use of red eye reduction would reduce the battery life.
- **White Balance:** If photograph quality is not acceptable for indoor photographs, choose **Fluorescent** or **Tungsten** (standard light bulb) lighting to reflect the type of indoor lighting being used.

10.6.3 Creating ID Cards Using the Apple Deployable Camera

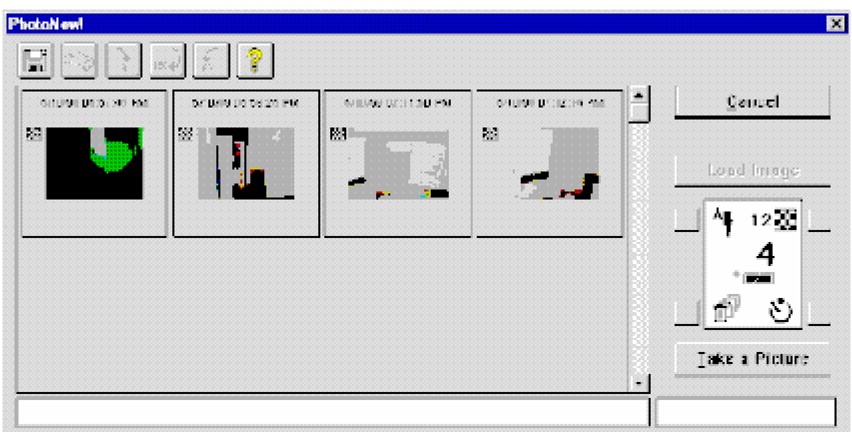
The following steps should be followed to create ID cards using the Apple deployable camera.

1. After having identified the persons for whom ID cards must be created, take all the photographs without connecting the camera to the laptop computer. The camera's memory must have enough space available to store the photographs you are taking; the camera's capacity is 16 photographs in high-resolution mode.

2. When all the photographs have been taken, connect the camera to the laptop computer using the cable provided.

3. In RAPIDS, open or create the family record for one of the persons whose photograph you have taken. Use the Create ID Card Navigator (see *Section 10.6.1* in this Training Guide).

4. When you reach the Modify Photo dialog box, click **Access Camera** in the bottom center of the Modify Photo dialog box. The PhotoNow! window will open. It will appear as shown below, except that it will not yet contain any photographs, and the toolbar buttons will all be active:



5. Click **Camera** on the toolbar; it is the second button from the left. Any images that are stored in the camera will appear as thumbnails. (In the above illustration, four thumbnails are shown).

6. Double-click the thumbnail that corresponds to the photograph of the person whose ID card you are currently creating. In a moment, the PhotoNow! window will close, and the photograph will appear in the Modify Photo window.

7. You may use the **Brightness** and **Contrast** controls on the right side of the window to fine tune the image by clicking and dragging the indicator arrows to the left or to the right.

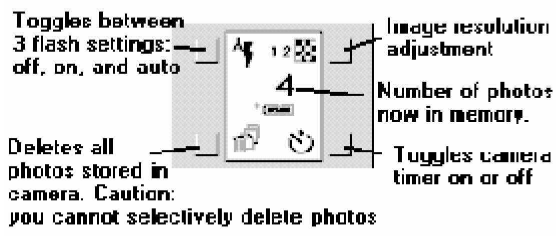
8. Click **OK** to advance to the next navigator screen. The Create ID Card navigator will walk the end user step-by-step through the printing of the ID.

9. Repeat steps 3-8 above for each person with photographs saved in the camera's memory.

10. After all ID cards have been created, delete the photographs from the memory.

10.6.4 Apple Camera Settings

The Apple deployable camera allows you to set some camera settings. You should only attempt to change these settings if the image quality is consistently poor. These options are located both on the camera to the right of the viewfinder, and on the right side of the PhotoNow! window that also displays the thumbnail images of the photographs that are stored on the camera. The following illustration shows you how the settings work, both on the camera and on the screen.



10.7 Desktop RAPIDS and Deployable RAPIDS Password Synchronization

In the RAPIDS environment, a unique six-digit DEERS site ID is established for each RAPIDS site regardless of the number of workstations installed. In the deployable RAPIDS environment, a unique six-digit DEERS site ID is established for each deployable RAPIDS laptop system.

Login IDs are generated for all personnel authorized to issue ID cards and are associated with a DEERS site ID. The RAPIDS system allows an individual user and his or her unique login ID to be assigned to multiple DEERS site IDs. With the implementation of the deployable RAPIDS systems, this practice has become more prevalent. Many of the users assigned to use the deployable RAPIDS systems are also users of RAPIDS desktop systems. In addition, multiple deployable RAPIDS systems were shipped to a single point of service (POS), and the POS established the same Login IDs for each Deployable RAPIDS system. As a result, as passwords expire users will be required to synchronize password changes on multiple desktop RAPIDS and Deployable RAPIDS systems.

The procedure below will allow a user to access his or her desktop RAPIDS and a deployable RAPIDS system using the same login ID and password. This will need to take place every time the user's password expires.

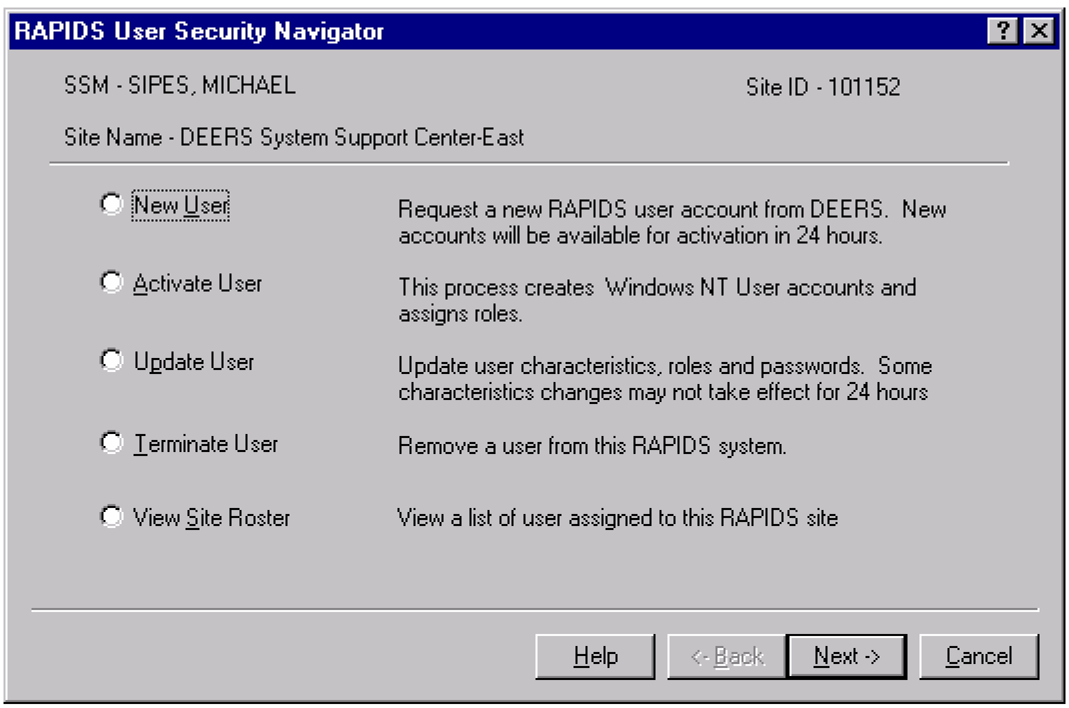
Note: This process can also be used to synchronize the desktop RAPIDS password to match the deployable RAPIDS system password. In step one, sign on to the Deployable RAPIDS system and in step two, synchronize the desktop password.

11. Ensure that the user knows his or her current DEERS password. This can be done by making sure the user can log in to the desktop RAPIDS system or one of the deployable RAPIDS systems and open a family record. If unsuccessful, contact the D/RAC / D/RSC-E / DSO-A for assistance.

12. Have the user log in to the next deployable RAPIDS system for which he or she has a valid login ID using the same password previously used successfully on that particular deployable RAPIDS system. This may or may not be the same password that successfully opened a family in step one. If unsuccessful, contact the D/RAC / D/RSC-E / DSO-A for assistance.

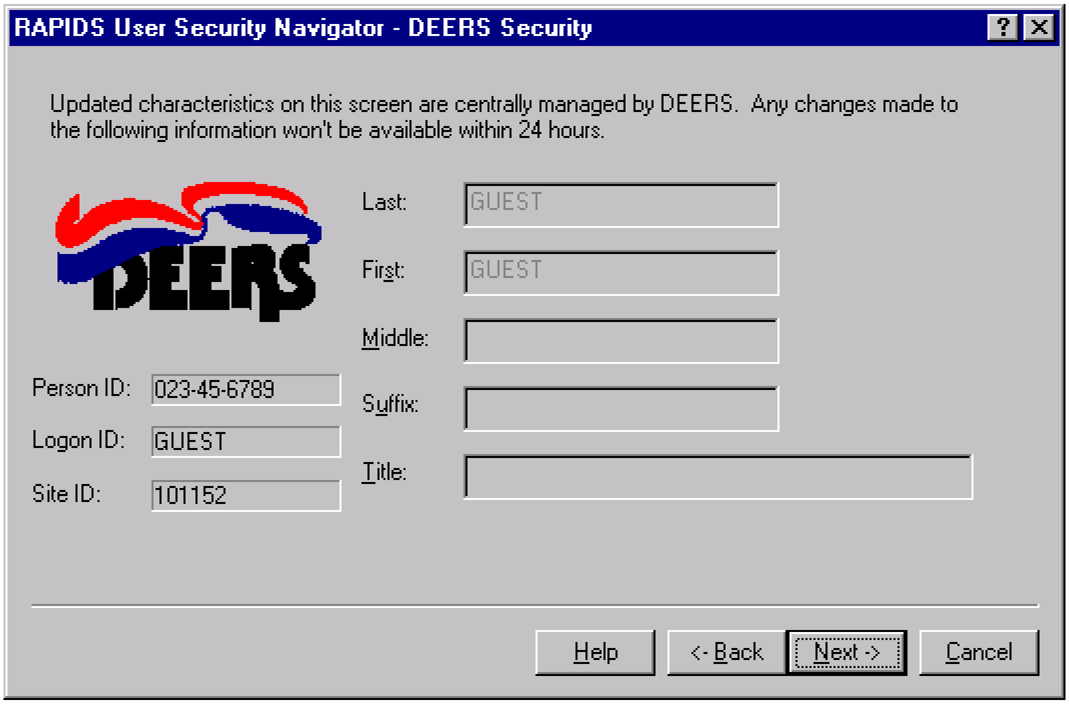
13. Open RAPIDS.

14. Highlight and select **Tools**. Then, click **User Administration**. The *RAPIDS User Security Navigator* screen will appear.

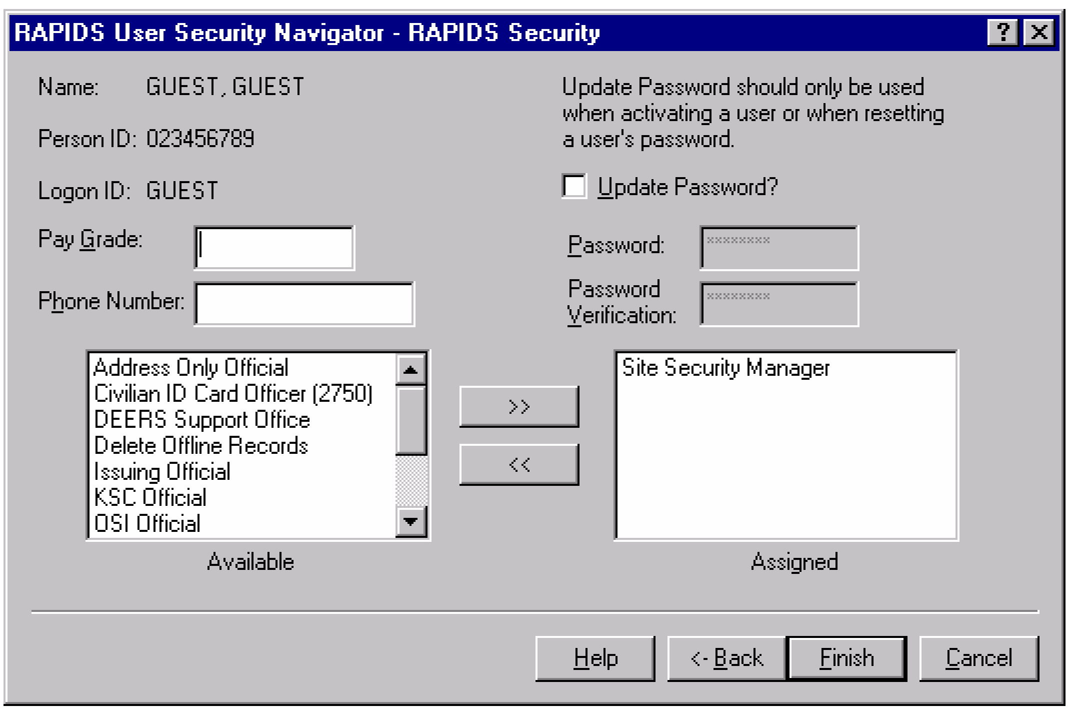


15. Select **Update User,** and then select **Next**. *The RAPIDS User Security Navigator - Update User* screen will appear with a list of valid users.

16. Select the appropriate user, and then select **Next**. The *RAPIDS User Security Navigator – DEERS Security* screen will appear.



17. Verify the user's name, and select **Next**. *The RAPIDS User Security Navigator - RAPIDS Security* screen will appear.



18. Click on the box labeled **Update Password?**

19. Type the new password that matches the system from which the user opened a family in step one in the **Password** box. Retype the same password in the **Password Verification** box and click **Finish**. This will synchronize the passwords.

20. Direct the user to log off and then log back on to the deployable RAPIDS system using the newly synchronized password.

21. Open RAPIDS and verify that a family can be opened.

Note: At sites with multiple deployable RAPIDS systems, steps two through 11 may need to be repeated for each deployable laptop in order to synchronize all systems.

10.8 Deployable Data Storage and Transmission

When you are using a desktop (non-deployable) workstation, any records in offline storage are automatically sent to DEERS every 30 minutes, as long as your workstation maintains its connection to DEERS. Because the DEERS communication status to deployable systems is so uncertain, there is no automatic transmission process for deployable RAPIDS. Users of deployable RAPIDS must manually instruct RAPIDS to send the records in the offline repository to DEERS. In addition, deployable users must make the following decision, based upon the anticipated availability or unavailability of communications.

- Should the records all be kept in offline storage because communications will be available within a reasonable period?
- Should the records be saved in an archive file that can be sent to a non-deployable RAPIDS site, which will in turn transmit the records to DEERS?

Three menu bar commands enable both deployable and desktop RAPIDS users to perform the following functions.

1. **File|Repository|Upload** menu command allows deployable RAPIDS users to transmit any family records in the offline storage repository to DEERS. **Uploading** is the feature by which a site with offline records (and the ability to connect to DEERS) can save their stored offline records to DEERS. An example of this is a Guard/Reserve site using its laptop in the field (in deployed mode) when no communications is available. The unit could then return to its home site (where communications is available) and upload all its offline records to DEERS.

2. **File|Repository|Offline|Export to File** menu command combines all family records that are currently contained in the offline repository into an archive file. You can choose to save on the deployable RAPIDS hard drive or to a 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. Exporting allows a site (with no communications) to save offline records elsewhere (e.g., floppy disk). A site with communications to DEERS can import the data from the floppy disk. Ships with no communications to DEERS are using this option. These ships can export their records to a floppy disk and take them to a desktop RAPIDS ID Card facility that can import their records using the step below.

3. **File|Repository|Offline|Import from File** menu command reads the exported (archived) 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 transaction database's hard drive) to hold the records contained in the archive.

10.8.1 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) and the records then sent to DEERS. You do not need connectivity to DEERS in order to create an archive file.

1. Select **File|Repository|Offline|Export to File** from the menu bar. A popup window asks you to confirm that you want to export your offline records. Click **Yes**. A standard Windows Save As… dialog box will open.
2. Save the archive to 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 before you boot up deployable RAPIDS, so Windows can detect it. Saving the archive on a floppy disk gives you the option of giving it to a desktop RAPIDS site for transmission to DEERS.
3. Assign the archive file a name by typing the name into the File name edit box. The default extension is .roa.
4. Click **Save**. If a file is too large to fit on one floppy disk, the user will be prompted to insert another floppy.

10.8.2 Importing an Archive File into Offline Storage

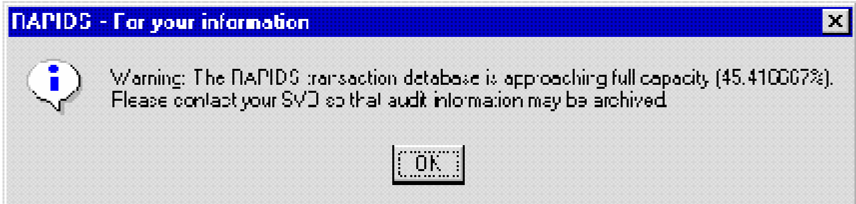
Once RAPIDS storage repository data has been exported to an archive file, it can then be imported back into offline storage. An example of this is to export data from deployable RAPIDS and import it to a desktop RAPIDS workstation, so that the data can be forwarded to DEERS. You do not need connectivity to DEERS in order to read the contents of an archive file into offline storage.

1. Select **File|Repository|Import from File** from the RAPIDS menu bar. The standard Windows NT Open window opens.
2. Select 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 **Open**. A popup window will notify you that the import was successful; click **OK** to close the notification popup.

Note: When an archive is read into offline storage, records from the archive that duplicate records already contained in offline storage are not "dropped." This can cause duplication of records in offline storage.

10.8.3 Deployable RAPIDS Limits for Size of Offline and Audit Trail Database

If you see the warning message shown below when you attempt to log in to deployable RAPIDS, your system's offline storage repository is full beyond the warning threshold that you (or another user of this deployable RAPIDS system) 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.

- **Connect and export the records to DEERS:** When the records are transmitted to DEERS, the storage repository on your laptop computer is emptied automatically. After offloading records, you can delete audit trail data as necessary.
- **Set the warning threshold higher:** In the ***Databases*** tab of the **Tools|Configuration** menu section, click **Advanced** near the top (in the **Transaction Database** section). Adjust the percentage that appears in the bottom (in the **Advanced Settings** section).

11 High Volume RAPIDS

11.1 Introduction

Some sites, such as those who routinely process recruits, have a requirement to produce large numbers of cards in a short period of time. This section supports sites that are configured as "High Volume." Personnel offices that produce and issue a large number of ID cards to military members in a relatively short period of time use High Volume RAPIDS. The High Volume configuration is generally used at Uniformed Services reception centers. The High Volume RAPIDS features give sites that are equipped with a duplex printer (such as an HP LaserJet 5 with the duplex option) an enhanced ability to produce ID cards more quickly than would be possible without the High Volume features. High Volume RAPIDS provides this enhanced capability using the following three shortcuts.

- Data is supplied for an entire group of sponsors from the service's personnel management information system (MIS). The records do not have to be entered into RAPIDS one item at a time by the RAPIDS clerk. RAPIDS clerks instead choose the sponsor's name from a list, capture the ID photo and fingerprint, and print the card.
- Records are not saved to DEERS as they are being processed. Instead, they are saved to offline storage on the RAPIDS transaction database, even when communications with DEERS is available. Offline records are saved from the RAPIDS server to DEERS by an automatic process that occurs every 30 minutes. This results in faster creation of ID cards.
- The actual printing of ID cards is faster because High Volume RAPIDS does not require a pause while the RAPIDS clerk reinserts the cardstock to print the back of the card. The RAPIDS clerk can load several blanks at once into the manual sheet feeder, producing many cards without pause.

This documentation supplements the RAPIDS 5.x Training Guide and assumes that the VO is already familiar with the use of the standard RAPIDS software. Initial training of the High Volume system should include reviewing the following scenarios from *Section 7*.

- Add a new Family to DEERS.
- Add Family Members to Sponsor.
- Separate Sponsor from Active Duty and Add to Guard/Reserves.
- Activate a Guard/Reserve Sponsor.
- Deactivate a Guard Reserve Sponsor.
- Terminate a Dependent child that is becoming a Sponsor.
- Transfer Guard/Reserve Sponsor from One Branch of Service to Another.
- Create DD Form 1172.
- Create ID Card.

The High Volume RAPIDS features are all accessed from the **File** option on the RAPIDS menu bar. The main High Volume feature is the High Volume Navigator, which is launched by the **File|Open Family From|Mass Issue Repository** command. This navigator guides you through the process of creating ID cards and/or Smart Cards using High Volume RAPIDS. This section contains detailed instructions for the High Volume Navigator and for the commands and dialog boxes that are used to move the service-provided beneficiary records into and out of RAPIDS so that your "pick list" is kept current.

11.2 Importing Records into High Volume RAPIDS

The source of most records that will be imported into High Volume RAPIDS is a data file created from the service's personnel management information system. However, it may sometimes be necessary for a user to import individual sponsor records into High Volume RAPIDS from DEERS, from the PDF417 bar code on the Uniformed Services ID card, or the CAC chip. The subsections below contain instructions for importing records from all possible sources.

In order to successfully read a new batch of records from the service's personnel system into High Volume RAPIDS, the data file that contains the records may be sent via file transfer protocol (FTP) from the personnel MIS to the RAPIDS server at your server site.

Once the data file has been copied to the RAPIDS server via FTP or disk, use the following procedure.

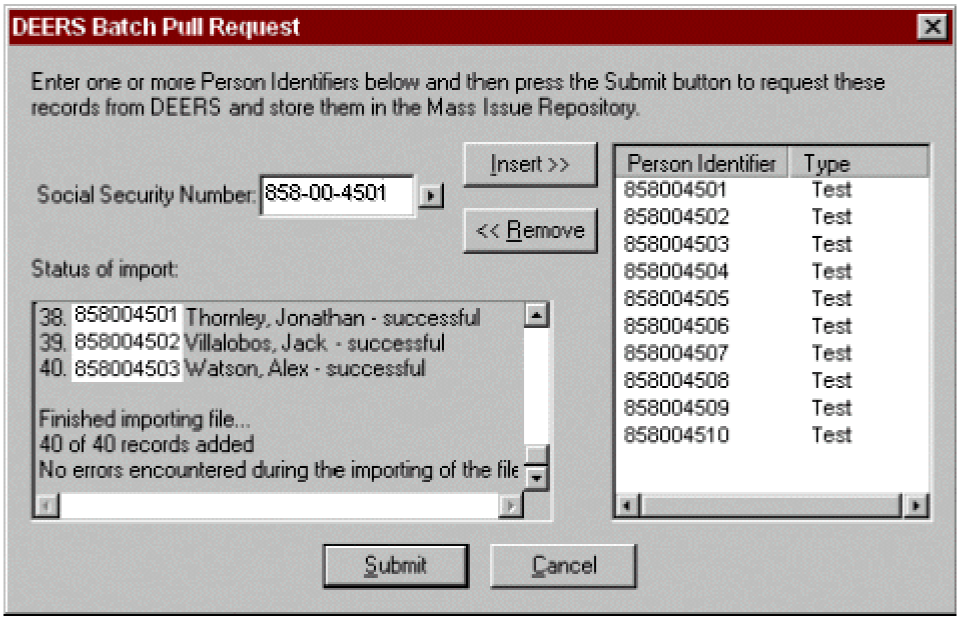
11.2.1 Importing Multiple Sponsor Records from FTP or Disk

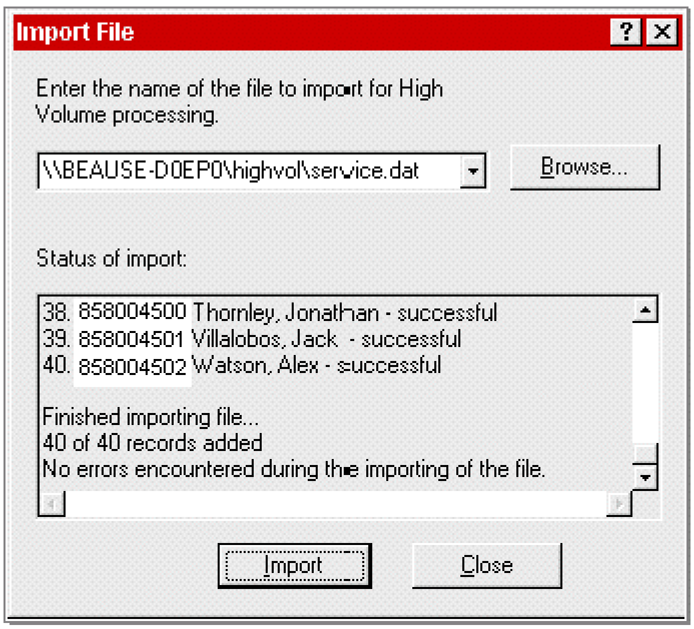
1. From the menu bar, select **File|Repository|Mass Issue|Service Personnel**. The Import File window opens. As shown in the following illustration, the default folder that appears in the text box is **highvol**.

2. If the folder path and file names are not correct for the file you wish to import, click on the right end of the text box to choose the correct path and file name from the choice list; or click **Browse** to navigate to the correct file.

3. Once you are certain the correct file is displayed in the top text box, click **Import**. Status messages will scroll in the Status of import: box. The following illustration shows you how the status messages conclude when the import has been successful. If unsuccessful, note that you can use the scrollbar to review the individual status of each record that was included in the data file.

4. Click **Close** to close the Import File window. Now, when you select the **Family|Open Family From…|Mass Issue Repository** command, all the records you just imported will be added to any records that already existed in the Mass Issue Records list.





Note: This procedure will not overwrite any records that were already in the Mass Issue Records list.

11.2.2 Importing Individual Sponsor Records from DEERS

1. From the menu bar, select **File|Repository|Mass Issue|Import From DEERS**. The DEERS Batch Pull Request window, shown by the following illustration.

2. In the Social Security Number text box, type the SSN of the first beneficiary whose record you want to add to the Mass Issue Records list. You can click on the right end

of the text box to choose from among other Person Identifier (PID) types, if the sponsor(s) you are adding have a PID other than a SSN.

3. Click **Insert**. The PID that you typed will appear in the text box on the right side of the window.

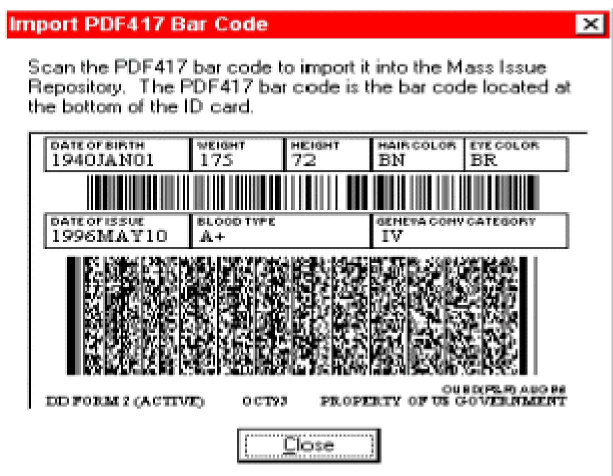
4. Repeat steps 2 and 3 for any other beneficiaries whose records you want to import from DEERS into the Mass Issue Records list. The list size is not limited by the size of the text box; as you add more records than can be seen at once, RAPIDS will automatically add a vertical scroll bar.

   To remove a record that you have mistakenly added to the list on the right side of the window, click the record in the list, then click **Remove**.

5. When you are finished creating the list, click **Submit**. Status messages will scroll in the Status of import: box. The illustration shows you how the status messages conclude when the import has been successful. If unsuccessful, note that you can use the scrollbar to review the individual status of each record that was included in the list.

11.2.3 Importing Individual Sponsor Records from PDF417 Bar Code on ID cards.

1. From the menu bar, select **File|Repository|Import From|PDF417 Bar Code**. The Import PDF417 Bar Code window opens, as shown here:



2. Scan the PDF417 bar code; it is the larger of the two bar codes on the back of a sponsor's standard ID card. Remember that in order to scan the PDF417 bar code, a bar code reader that is capable of scanning the PDF417 bar code is required.

3. If the import is successful, the message “Import successful” appears, and when you open the Mass Issue Records list it will include the record. If the import is not successful, the pop-up window will read **Import not successful. Please try again**.

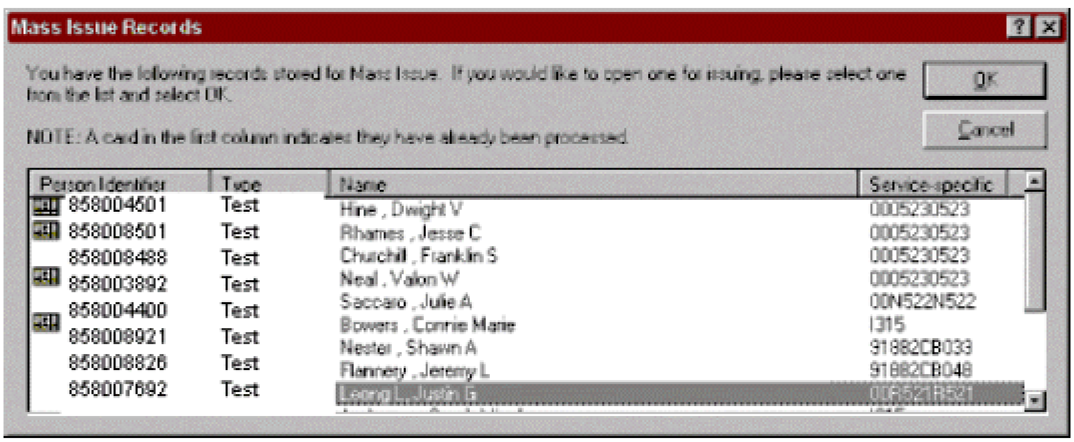
11.3 Creating ID Cards with High Volume RAPIDS

This section provides instructions for the High Volume Navigator, which you use to produce cards using the High Volume RAPIDS features. In order to use the High Volume Navigator, the following things must be true:

- You have imported records into the Mass Issue Records list.
- Your RAPIDS workstation is configured to use a duplex printer. If your workstation is not so configured and you are unsure of how to accomplish this, call the D/RAC / D/RSC-E / DSO-A for assistance.
- In order to produce Smart Cards, the workstation must be equipped with a Smart Card printer.

The following subsections contain the step-by-step instructions for using the High Volume Navigator.

1. To launch the High Volume Navigator, select **File|Open Family from…|Mass Issue Repository** from the menu bar. The Mass Issue Records window opens, as shown here.



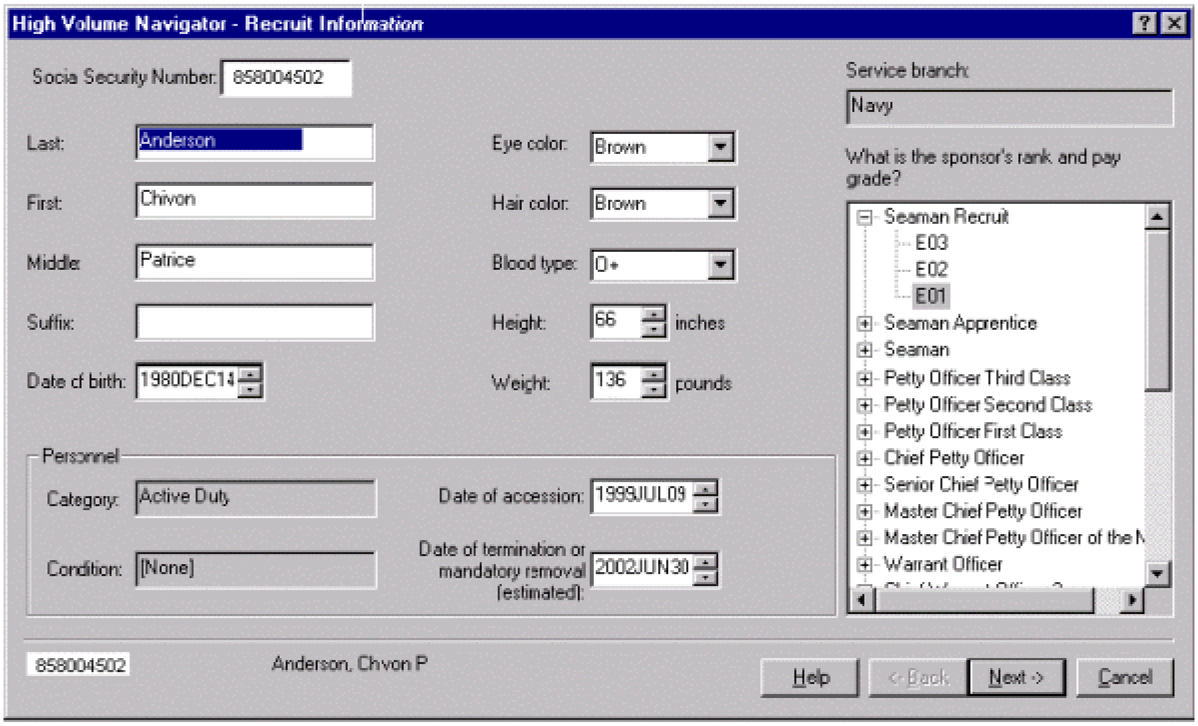
2. Double-click the line of data that corresponds to the beneficiary for whom you need to create a card. Scroll if necessary to find the beneficiary's name. When you double-click a record, you will advance to the Recruit Information window.

   Here are three hints to help you find the correct record quickly:

- **You can sort the records numerically by PID by clicking on the "Person Identifier" column heading. Then, type the first four characters of the PID of the beneficiary for whom you are creating an ID card or Smart Card, the list will automatically scroll closer to the beneficiary's record with each number you type until finally, you will see the record. This "auto-scroll" feature does not work for any columns except for the Person Identifier column.**
- **You can sort the records in the list alphanumerically according to the data in any of the four columns, by clicking on the column heading according to which you want the list sorted. For instance, to sort the list alphanumerically by last names, point and click the "Name" heading.**

- **Those records for which cards have already been created are indicated by the presence of a card icon in the far-left column. In the illustration that appears above, four of the beneficiaries whose records are showing in the list have had a card created for them using High Volume RAPIDS.**

After you have selected a beneficiary in the Mass Issue Records window and clicked **OK**, the Recruit Information window appears, as shown here.



The Recruit Information window contains all the information needed in order for you to produce a card for the beneficiary. You should verify the accuracy of this information by reading it back to the beneficiary, and making any corrections as necessary (see Note).

When you have verified that all the information on this screen is correct, click **Next**, located near the bottom right of the window, to advance to the Modify Photo window.

Note: You cannot correct the beneficiary's PID, personnel category, personnel condition, or service branch in this screen. You must instead make these corrections by retrieving the record from DEERS and making the necessary changes and updates online.

From this point forward, the High Volume Navigator functions in the same way as the Create Card Navigator with regard to taking the photo, capturing the fingerprint, and requiring that you provide a reason for terminating any previous ID card.

If your workstation is only configured to produce Smart Cards but not standard ID cards, steps one through four of the following instructions do not apply.

When you have captured both the ID photo and the fingerprint, the Print ID Card window appears, as shown here.

3. If you want to print only a Smart Card for this beneficiary, click **Skip** in the lower right corner of the window, and you will advance to the Print Smart Card window. The Smart Card is printed the same way when you are using High Volume RAPIDS as when you are using RAPIDS without the High Volume options.

   Note: If the workstation you are using is not configured to print Smart Cards, **Skip** is instead labeled **Cancel** and will close the navigator, returning you to the Mass Issue Records window.

- If your workstation is configured to print Smart Cards: **The Print Smart Card window will open; go to step 5 of this instruction.**
- If your workstation is not configured to print Smart Cards: **The Mass Issue Records window will open, allowing you to select the next beneficiary.**

4. To print a standard ID card for this beneficiary, review the information on both the front and back sides of the card, as shown in the Print ID Card window, to ensure its accuracy. If any of the information is incorrect, click **Back** to move backward one screen at a time to find the error and make the correction.

5. If a stack of cardstock is not already loaded, follow the instructions on the Print ID Card window to load the correct cardstock into the printer's duplex feeder. It is anticipated that in most high-volume scenarios, you will need to create a large number of cards for sponsors of the same type; therefore you should be able to load the feeder with a stack of cardstock.

   Note: To load the cardstock place the DD Form 2 (ACTIVE) in the printer's multipurpose tray, green side face down, with the top edge away from the printer, and the left side aligned with the left guide.

6. Click **Print**. The front and backsides of the ID card will be printed.

7. If you do not want to print a Smart Card for this beneficiary, click **Skip** in the lower right corner of the window. You will return to the Mass Issue Records window, where you can select the next beneficiary.

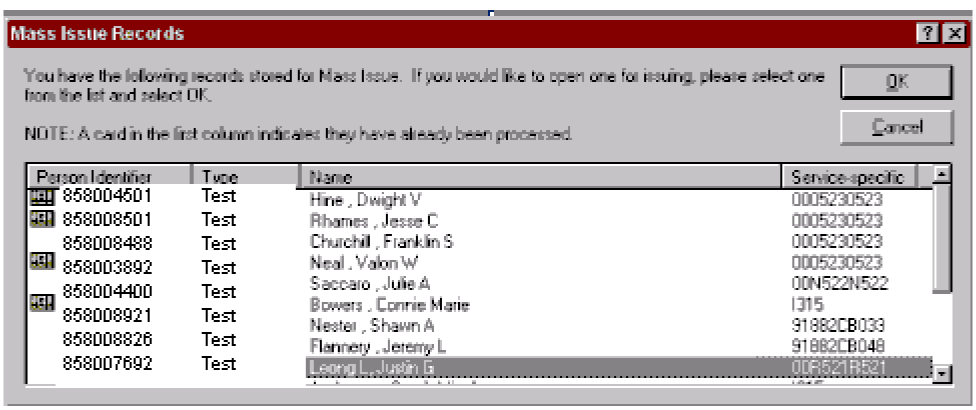
8. If you want to print a Smart Card for this beneficiary, fill the requested information in to the text boxes provided, and ask the beneficiary to type and confirm his or her PIN using the numeric keypad. Click **Print** to print the Smart Card and return to the Mass Issue Records window.

   Note: When printing a card, a message will appear asking if the card printed correctly. Please wait until the card has completed printing before answering the question on your screen.

11.4 Deleting Records from High Volume RAPIDS

You should delete any processed records from the Mass Issue Records list after you have processed an entire batch, in order to clear the list for the next batch of records you import. Additionally, you may want to periodically delete processed records during High Volume card production, so that it is easier to find the remaining records that have already been processed. In order to delete one or more record(s) from the Mass Issue Records list:

1. From the menu bar, select **File|Repository|Mass Issue|Delete** to open the Mass Issue Records delete window, as shown here.



2. Select the records you want to delete by clicking on them so they are highlighted. You can click the column heading of your choice to sort the list, and then use standard Windows selection methods to choose more than one record at a time. There are two ways to select multiple records:

3. **To select a continuous range of records:** Click to highlight the first record in the range, then hold down SHIFT and click the last record in the range.

4. **To select non-continuous records**: Click to highlight one of the records you wish to select for deletion, then hold down CTRL while clicking on subsequent records.

5. When you have highlighted all the records you want to delete, click DELETE near the upper right corner of the window. The records will be deleted from the Mass Issue

Records list. If you discover that you have deleted records in error, you will now have to import them again from your service's personnel system in order to issue ID cards to those beneficiaries using High Volume RAPIDS.

6. Click **Close** to close the window.

Appendix A - Quick Reference Guide

Site Workstation Information

Workstation #1 IP:	###.###.###.###	Workstation #1 Serial #:	
Workstation #2 IP:	###.###.###.###	Workstation #2 Serial #:	
Workstation #3 IP:	###.###.###.###	Workstation #3 Serial #:	
Workstation #4 IP:	###.###.###.###	Workstation #4 Serial #:	
Workstation #5 IP:	###.###.###.###	Workstation #5 Serial #:	
Workstation #6 IP:	###.###.###.###	Workstation #6 Serial #:	

Server Site Information:

Server Site Name	Phone #	P.O.C.

Note: If your site has more than six workstations, please complete and print a second page.

Field Rep Name:		**Phone Number:**	

Help Desk

CONUS, Alaska, Hawaii, Panama, Virgin Islands, Cuba, and Puerto Rico

DEERS/RAPIDS Assistance Center
(800) 3-RAPIDS or (800) 372-7437 or (800) 828-3184
DSN: 761-6953
Hours: M-F 0700 EST - 2000 EST | Sat-Sun 0800 EST - 1700 EST (except U.S. Govt. 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 (Landstuhl, Germany)
Comm: 011-49(0)-6371-86-7365
DSN: 486-7365
Comm Fax: 011-49(0)-6371-86-7672
DSN Fax: 486-7672
Hours: M-F 0800 - 1700 Local Time (except U.S. Govt. holidays)

Western Pacific Theater

DMDC Support Office (DSO) – Asia/Pacific (Seoul, Korea)
Comm: 011-822-7914-6195
DSN: 724-6195
Fax 1: 011-822-795-1092 | Fax 2: 011-822-7914-6204
DSN Fax: 724-6204
Hours: M-F 0800 - 1700 Local Time (except U.S. Govt. holidays)

General Information

The **DEERS/RAPIDS Program Office (D/RPO)** is responsible for managing the DEERS/RAPIDS program. If you have questions about funding for relocation or comments concerning RAPIDS please contact:

Defense Manpower Data Center (DMDC)
Attn: DEERS/RAPIDS Program Office
1600 Wilson Boulevard, Suite 400
Arlington, Virginia 22209-2593
Comm: (703) 696-2000/2001
DSN: 426-2000/1
Fax: (703) 696-1461
DSN Fax: 426-1461

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
Fax: (831) 373-1228

DSO Research and Analysis (R&A)

Contact DSO R&A for assistance with record problems or data discrepancies:

Comm: (800) 361-2508
DSN: 878-3522/3523

Beneficiaries with questions or problems concerning DEERS enrollment or claim denials:

DEERS Beneficiary Telephone Center (DBTC)
California Only: (800) 334-4162
Alaska & Hawaii: (800) 527-5602
All Other States: (800) 538-9552
Hours: M-F 0600 PST - 1530 PST (except U.S. Govt. holidays)

VOs who have a DEERS login ID and password and need to verify the eligibility of sponsors and family members should please contact:

DEERS Eligibility Telephone Center (DETC)
Comm: (800) 368-4416 or (800) 336-0289
DSN: 837-6299
Hours: M-F 0600 PST - 1600 PST (except U.S. Govt. holidays).

Appendix A - Quick Reference Guide – Server Site

Server IP Address:	###.###.###.###	**Server Serial #:**	

Site Workstation Information

Workstation #1 IP:	###.###.###.###	Workstation #1 Serial #:	
Workstation #2 IP:	###.###.###.###	Workstation #2 Serial #:	
Workstation #3 IP:	###.###.###.###	Workstation #3 Serial #:	
Workstation #4 IP:	###.###.###.###	Workstation #4 Serial #:	
Workstation #5 IP:	###.###.###.###	Workstation #5 Serial #:	
Workstation #6 IP:	###.###.###.###	Workstation #6 Serial #:	

Remote Site Information:

Remote Site Name	Phone #	P.O.C.

Note: if your site has more than 4 remote sites or more than six workstations, complete and print a second page.

Field Rep Name:		**Phone Number:**	

Help Desk

CONUS, Alaska, Hawaii, Panama, Virgin Islands, Cuba, and Puerto Rico

DEERS/RAPIDS Assistance Center
(800) 3-RAPIDS or (800) 372-7437 or (800) 828-3184
DSN: 761-6953
Hours: M-F 0700 EST - 2000 EST | Sat-Sun 0800 EST - 1700 EST (except U.S. Govt. 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 (Landstuhl, Germany)
Comm: 011-49(0)-6371-86-7365
DSN: 486-7365
Comm Fax: 011-49(0)-6371-86-7672
DSN Fax: 486-7672
Hours: M-F 0800 - 1700 Local Time (except U.S. Govt. holidays)

Western Pacific Theater

DMDC Support Office (DSO) – Asia/Pacific (Seoul, Korea)
Comm: 011-822-7914-6195
DSN: 724-6195
Fax 1: 011-822-795-1092 | Fax 2: 011-822-7914-6204
DSN Fax: 724-6204
Hours: M-F 0800 - 1700 Local Time (except U.S. Govt. holidays)

General Information

The **DEERS/RAPIDS Program Office (D/RPO)** is responsible for managing the DEERS/RAPIDS program. If you have questions about funding for relocation or comments concerning RAPIDS please contact:

Defense Manpower Data Center (DMDC)
Attn: DEERS/RAPIDS Program Office
1600 Wilson Boulevard, Suite 400
Arlington, Virginia 22209-2593
Comm: (703) 696-2000/2001
DSN: 426-2000/1
Fax: (703) 696-1461
DSN Fax: 426-1461

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
Fax: (831) 373-1228

DSO Research and Analysis (R&A)

Contact DSO R&A for assistance with record problems or data discrepancies:

Comm: (800) 361-2508
DSN: 878-3522/3523

Beneficiaries with questions or problems concerning DEERS enrollment or claim denials:

DEERS Beneficiary Telephone Center (DBTC)
California Only: (800) 334-4162
Alaska & Hawaii: (800) 527-5602
All Other States: (800) 538-9552
Hours: M-F 0600 PST - 1530 PST (except U.S. Govt. holidays)

VOs who have a DEERS login ID and password and need to verify the eligibility of sponsors and family members should please contact:

DEERS Eligibility Telephone Center (DETC)
Comm: (800) 368-4416 or (800) 336-0289
DSN: 837-6299
Hours: M-F 0600 PST - 1600 PST (except U.S. Govt. holidays).

Appendix B - Field Service Representatives Map

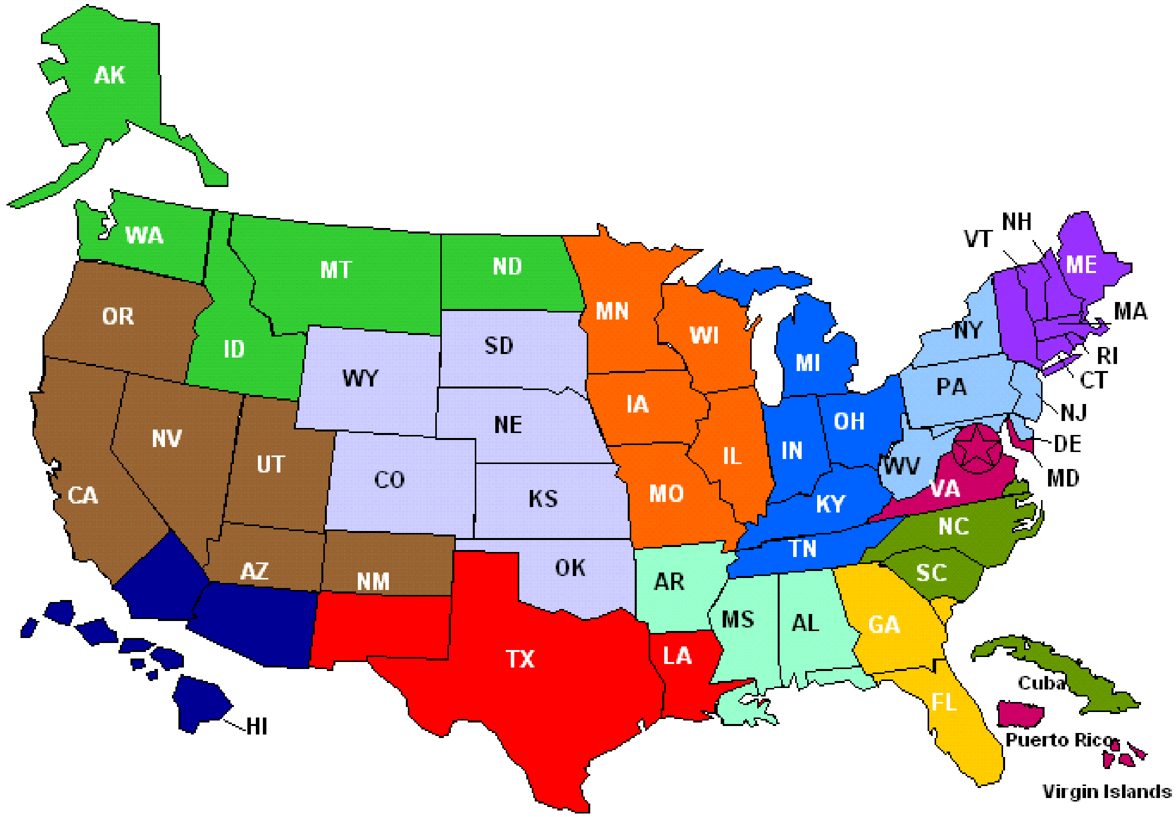
The subject map is on the following page.

Northwest (NW)
Joe Miller
DEERS/RAPIDS Field Rep
62nd MSS/DPMP
100 Main Street, Suite 1033A
McChord AFB, WA 98438
(253) 984-2553
DSN 382-2553
FAX (253) 984-3966
millerjb@osd.pentagon.mil

West (WC)
Lowell Huddleston
DEERS/RAPIDS Field Rep
DSO
400 Gigling Road
Seaside, CA 93955-6771
(831) 583-2500 ext. 308
DSN 878-3261
FAX (831) 373-1228
huddlell@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
robertbl@osd.pentagon.mil

Rocky Mountain (RM)
TBA
DEERS/RAPIDS Field Rep
TRICARE Central Region
Bldg. 1011, Specker Ave.
Ft. Carson, CO 80913
(719) 524-2619
DSN 883-2619
FAX (719) 556-7743



Manager, Field Operations
***Tina Roberts**
(703) 578-5245
robertp@osd.pentagon.mil

Field Rep Consultant
***Sangeeta Ryan**
(703) 578-5309
ryansd@osd.pentagon.mil

Field Rep Consultant
***Lou Leach**
(703) 578-5282
leachml@osd.pentagon.mil

Capital
***Jay Anderson**
(703) 578-5310
andersjs@osd.pentagon.mil

Northeast
***Suellen Black**
(703) 578-5211
blacksn@osd.pentagon.mil

*DEERS/RAPIDS
1600 N Beauregard Street
Alexandria, VA 22311
DSN 761-6953/7
FAX (703) 578-5325

Europe
John Connin, Manager
EDS US Hospital Kirchberg
West 6th Street
Building 3767206
66849 Landstuhl Germany
011-49-6371-921823
DSN 486-7365
FAX 011-49-6371-921831

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
milesr@usfk.korea.army.mil

Southwest (SW)
Bert Howard
DEERS/RAPIDS Field Rep
PASBA
1216 Stanley Road
Building 126, Suite 25
Ft Sam Houston, TX 78234
(210) 221-2636
DSN 471-2636
FAX (210) 221-9016
howardbl@osd.pentagon.mil

South (SO)
Cyndi Aviles
DEERS/RAPIDS Field Rep
314 MSS/DPMPS
1255 Vandenburg, Suite 116
Little Rock, AR 72099
(501) 987-8960
DSN 731-8960
FAX (501) 987-7932
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) 263-3938
DSN 693-3938
FAX (314) 263-2761
newettpa@osd.pentagon.mil

Great Lakes (GL)
Peter Purol, Jr.
DEERS/RAPIDS Field Rep
127th MSS/DPM
Building 304
Selfridge ANG Base, MI 48045
(810) 307-5625
DSN 273-5625
FAX (810) 307-6240
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
DSN 423-2481
FAX (717) 948-2531
seidenlr@osd.pentagon.mil

Gulf Coast (GC)
Fred Stark
DEERS/RAPIDS Field Rep
6 MSS/DPM
8011 Tampa Point Blvd.
MacDill AFB, FL 33621-5321
(813) 828-9714
DSN 968-9714
FAX (813) 828-2277
starkfh@osd.pentagon.mil

Southeast (SE)
Denise Hutchins
DEERS/RAPIDS Field Rep
43rd MSS/DPMPS
384 Maynard Street
Pope AFB, NC 28308-2374
(910) 394-4744
DSN 424-4744
FAX (910) 394-4747
hutchida@osd.pentagon.mil

FSR
Andrea Deshaye
DEERS/RAPIDS Field Rep
62nd MSS/DPMP
100 Main Street, Suite 1033A
McChord AFB, WA 98438
(253) 984-8458
DSN 382-8458
FAX (253) 984-3966
deshayaj@osd.pentagon.mil

Appendix C – Joint Uniformed Services Personnel Advisory Committee

Army (USA)

Cindy Sublett
HQDA (TAPC-PCO-IP)
Hoffman Building 2, Room 3S49
200 Stovall Street
Alexandria, VA 22332-0474
(703) 325-0202/4525
DSN: 221-8941/9590
FAX: (703) 325-4532
Jacqulin Hines (703) 325-4525
hinesj@hoffman.army.mil

Navy (USN)

LT Q Jones
Navy Personnel Command
PERS-332, Building 769
5720 Integrity Drive
Millington, TN 38055-3320
(901) 874-3466
DSN: 882-3466
FAX: (901) 874-2640
p332@persnet.navy.mil

Doris Perry
(901) 874-3467
DSN: 882-3467
p332b@persnet.navy.mil

Air Force (USAF)

Mr. George Hoback
HQ AFPC/DPSFR
550 C Street W.
Suite 37
Randolph AFB, TX 78150-4739
(210) 565-2089/2467
DSN: 665-2089/2467
FAX: (210) 565-2543
george.hoback@afpc.randolph.af.mil

Marine Corps (USMC)

Ms. Mary Stroz
HQ USMC Manpower and Reserve Affairs
CODE: MRP-1
3280 Russell Road
Quantico, VA 22134
(703) 784-9529/9530/9531/9532
DSN: 278-9529/9530/9531/9532
FAX: (703) 784-9827
StrozM@manpower.usmc.mil

Ms. Norma Reiter
Nlreiter@manpower.usmc.mil

Coast Guard (USCG)

CWO2 Connie K. Rapp
DEERS/RAPIDS Project Officer
Commandant (G-WPM-2)
(202) 267-2257
FAX: (202)267-4823
crapp@comdt.uscg.mil

Public Health Service (PHS)

Mr. Norman Chichester
Officer Development Branch P
Parklawn Building, Room 4-35
5600 Fishers Lane
Rockville, MD 20857
(301) 594-3393
FAX: (301) 594-2711
nchichester@psc.gov

National Oceanic And Atmospheric Administration (NOAA)

Mr. Steve Eisenberg
SSMC #3, Room 12100
1315 East West Highway
Silver Spring, MD 20910
(301) 713-3453 (ext. 102)
FAX: (301) 713-4140
steve.eisenberg@noaa.gov

OUSD Reserve Affairs (OUSD/RA)

COL James Scott
Guard and Reserve Program Manager DEERS/RAPIDS
OASD/RA (M&P)
1500 Defense Pentagon
Washington, DC 20301-1501
(703) 693-7490
FAX: (703) 695-3659
jscott@osd.pentagon.mil

Army National Guard (USARNG)

Ms. Judith Mitchell
ARNG Readiness Center
ATTN: NGB-ARP-S
111 South George Mason Drive
Arlington, VA 22204-1382
(703) 607-9194
DSN: 327-9194
FAX: (703) 607-7184
judith.mitchell@ngb.army.mil

Army Reserve (USAR)

MAJ Tabatha Dunlap
Office of the Chief Army Reserve
Attn: DAAR-PER-H
Jefferson Plaza 2, Suite 1100
1421 Jefferson Davis Highway
Arlington, VA 22202-3259
(703) 601-3530
DSN: 329-3530
FAX: (703) 601-3501
melody.maynard@ocar.army.pentagon.mil

Army Reserve-FORSCOM (USAR)

Ms. Dorothy Howell
HQ FORSCOM
ATTN: AFAG-PSS-O, Building 200
Fort McPherson, GA 30330-1062
(404) 464-6252
DSN: 367-6252
FAX: (404) 464-6830
howelldo@forscom.army.mil

Army Reserve-USARC (USAR)

MAJ David Moilien
HQ USARC, ATTN: AFRC-PRF (DEERS/RAPIDS)
1401 Deshler Street
Fort McPherson, GA 30330-2000
(404) 464-8946
FAX: (404) 464-8950
DSN: 367-8946
david.moilien@usarc-emh2.army.mil

Navy Reserve (USNR)

Chief Ekart
Commander Naval Forces, CODE: N12B
4400 Dauphine Street
New Orleans, LA 70146-5000
(504) 678-6133
FAX: (504) 678-0629
DSN: 678-6133
DSN FAX: 678-0629
ekart@cnrf.nola.navy.mil

Air National Guard (USANG)

Tammy J. Bump, MSgt, USAF
Air National Guard DEERS/RAPIDS Project Officer
ANG/DPFOC
1411 Jefferson Davis HighwayArlington, VA 22202-3231
DSN: 327-3920
FAX DSN: 327-1066
tammy.bump@ngb.ang.af.mil

Air Force Reserve (USAFR)

LtCol Dave Percich
HQ, USAF/REPP
1150 Air Force Pentagon
Washington, DC 20330-1151
(703) 588-6002
FAX: (703) 588-8444/8
DSN: 425-6002
david.percich@pentagon.af.mil

Air Reserve Personnel Center (ARPC)

(20 yr. Letters/Survivor Benefits)
(800) 525-0102 x227
DSN: 926-6438 (Rhonda)
DSN: 926-6576 (Darrel Grunius)

Marine Corps Reserve (USMCR)

CWO-2 Robin C Porche
Commander, MARFORRES, Code 7AA
4400 Dauphine Street
New Orleans, LA 70146-5440
(504) 678-5604
FAX: (504) 678-1082
DSN: 678-5604
DSN FAX: 678-1082
porcherc@mfr.usmc.mil

Coast Guard Reserve (USCGR)

LT Cassandra Johnson
Commandant (G-WTR-1)
2100 Second Street, SW
Washington, DC 20593
202-267-0569
FAX: (202) 267-4243
cjohnson@comdt.uscg.mil

Appendix D – Joint Uniformed Services Medical Advisory Committee

Army (USA)

Mr. Alton Clark
U.S. Army Medical Command
ATTN: MCHO-CL-P
2050 Worth Road
Fort Sam Houston, TX 78234-6000
(210) 221-6113/6631
DSN: 471-6113/6631
FAX: (210) 221-6630
alton.clark@cen.amedd.army.mil

Navy (USN)

Mr. Skip Katon
Department of the Navy
Bureau of Medicine and Surgery (Attn: MED-31BAS)
2300 E. Street, NW
Washington, DC 20372-5301
(202) 762-3144
DSN: 762-3144
FAX: (202) 762-3743
fakaton@us.med.navy.mil

Air Force (USAF)

Mr. Michael Harrison
(Health Benefits and Policy Division) HQ USAF-SGMA
110 Luke Avenue, Suite 400
Bolling AFB, DC 20332-7051
(202) 767-4699
FAX: (202) 404-7366
michael.harrison@usafsg.bolling.af.mil

Coast Guard (USCG)

Mr. Terry Strickland
Commandant (G-WKH-3)
2100 Second Street, SW
Washington, DC 20593-0002
(202) 267-0835
FAX: (202) 267-4346/4685
wstrickland@comdt.uscg.mil

Uniformed Services Family Health Plan (USFHP)

Mr. Earl Hanson
OASD (HA) TMA/MHSO/SP&D
Skyline 5, Suite 810
5111 Leesburg Pike
Falls Church, VA 22041-3206
(703) 681-1757/1742
DSN: 761-1757
FAX: (703) 681-3678
earl.hanson@tma.osd.mil

Public Health Service (PHS)

Dr. Alvin Abrams
Chief, Beneficiary Medical Branch - DMP
Parklawn Building, Room 4C06
5600 Fishers Lane
Rockville, MD 20857
(301) 594-6330
FAX: (301) 594-2973
aabrams@psc.gov

National Oceanic and Atmospheric Administration (NOAA)

CAPT Michael Vitch
Director, Office of Health Services
NOAA Office of Marine and Aviation Operations
Room 12734, 1315 East-West Highway
Silver Spring, MD 20910-3282
(301) 713-3440 (ext. 186)
FAX: (301) 713-2887
michael.vitch@noaa.gov

Medical System (Technical)

Tri-Service
Tri-Service Medical Systems Support Center (TMSSC)
Help Desk
1-800-600-9333
(210) 536-4150
DSN: 240-4150

Service Tumor Registrar Consultants

Army

Ms. Judith Tryon
Certified Tumor Registrar
William Beaumont AMC
5005 N. Piedras Street
El Paso, TX 79920-5001
(915) 569-2106
DSN: 979-2106
Judith.Tryon@amedd.mil

Air Force

Ms. Betty Nielsen
Certified Tumor Registrar
49th Medical Group/SGOCR
280 1st Street
Holloman AFB, NM 88330-8273
(505) 572-3578
DSN: 572-3578
Betty.Nielsen@holloman.af.mil

Navy

Ms. Michelle Snyder
Certified Tumor Registrar
National Naval Medical Center
8901 Wisconsin Avenue
Bethesda, MD 20889-5000
(301) 295-5706
DSN: 295-5706

Appendix E - RAPIDS Acronyms

AD	Active Duty
AHSMC	Auburn Hills Service Management Center
API	Application Programming Interface
BRAC	Base Realignment and Closure
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
CMA	Certificate Management Authority
CONUS	continental United States
COTS	Commercial off the Shelf
CPS	Certification Practice Statement
CPU	central processing unit
CRL	Certificate Revocation List
DAV	Disabled Veterans
DD Form	Department of Defense Form
DEERS	Defense Enrollment Eligibility Reporting System
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/RPO	DEERS/RAPIDS Program Office
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
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
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
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/RPO for CONUS, Alaska, Hawaii, Panama, 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/RPO 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/RPO. 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.

1. Submit a written request to the D/RPO / 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.

2. Upon approval, the relocation contractor will contact you to determine what services and additional equipment will be required to complete your move.

3. The D/RPO will determine funding requirements. The D/RPO, 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/RPO.

4. The funding documentation should be submitted to the D/RPO. 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/RPO 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 Program Office
   1600 Wilson Blvd, Suite 400
   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/RPO / D/RSC.

- After notification by the D/RPO / 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/RPO. For additional information contact:

CONUS, Alaska, Hawaii, United States Virgin Islands, Cuba, and Puerto Rico

Defense Manpower Data Center
DEERS/RAPIDS Program Office
1600 Wilson Blvd, Suite 400
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/RPO 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/RPO 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

1. **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.

2. **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.

3. **Configuration Changes.** Movement of equipment that causes changes to the system's configuration will generate additional equipment costs, to be determined by the D/RPO during preliminary planning and included in the cost estimate.

4. **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/RPO initiates a Base-to-Base relocation, the D/RPO 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:

	Present	Proposed
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 SPO 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 x 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 x One) | FACILITY SECTION (Check x One)

Dental Clinic = D	_______	AAFES = S	_______	FINCTR w/Title III = FT	_______
Health Clinic = M	_______	AQCESS/CHCS = G	_______	Medical/Dental Rec = R	_______
Hospital = H	_______	Army Fin Off = F	_______	Tumor Registry = T	_______
Personnel Office = P	_______	Civ Person Off = C	_______	Other = Z	_______
Other = Z					

OPFAC, PAS, RUC or UIC code is ___________________________________.
*See Section II below, EQUIPMENT NOTE.

SAMPLE	FULL MAILING ADDRESS
Chief, Health Services	Point of Contract (title, not person's name)
**REMAINDER OF ADDRESS USCG Clinic, New Orleans	REMAINDER OF ADDRESS
Attn: Medical Records	
4640 Urquhart Street	
New Orleans, LA 70017-1010	

**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 x One)

ACTUR	_______	ARED	_______	DOLI	_______	OLGR	_______	RAPIDS	_______
AQCESS/CHCS	_______	DMRIS	_______	GIQD	_______	OLPU	_______	OTHER	_______

EQUIPMENT (Check x 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 Program Ofc.)

DEERS/RAPIDS Program Office
1600 Wilson Boulevard, Suite 400
Arlington, Virginia 22209-2593

V.

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: ____________________
Chief, Operations Branch

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:

1. Double-click the QWS3270 Application icon from the desktop.

2. 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.

3. 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.

4. The “Welcome to AHIPC” screen will be displayed. At the prompt, type **DEERS** and press **ENTER** to enter the DEERS database.

5. The “Welcome to CICS” screen will be displayed.

6. 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.

1. At the DMDC Security screen, enter your DEERS login ID and password. Enter **DOLI** at the “Tran ID” prompt and press **ENTER**.

2. 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**.

3. 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.

4. 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.

1. On the Security screen enter your DEERS login ID and password. Enter **PANO** at the “Tran ID” prompt and press **ENTER**.

2. 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**.

3. To do additional checks, type **CS** (Clear Screen) in the Action Field and repeat step two.

4. To sign off, type **SO** in the Action Field.

Appendix J – Removing a Card Jam at the End of the Laminate Roll

If the laminate becomes stuck to a card or jams inside the printer, the LCD Display will indicate that it is jammed (LAM JAM). Refer to the following steps and Figure 1, below, to clear the jam.

CAUTION! DO NOT TOUCH THE METAL LAMINATION SHIELD OR THE LAMINATION ROLLER. YOU WILL BURN YOURSELF!

1. Leave the power ON and open the printer's Top Covers, using the Cover Release Buttons and pulling each cover up and out.
2. Remove the Lamination Take-up Roll (the side with used laminate on it) from in between the two black Take-up Lamination Drive Hubs.

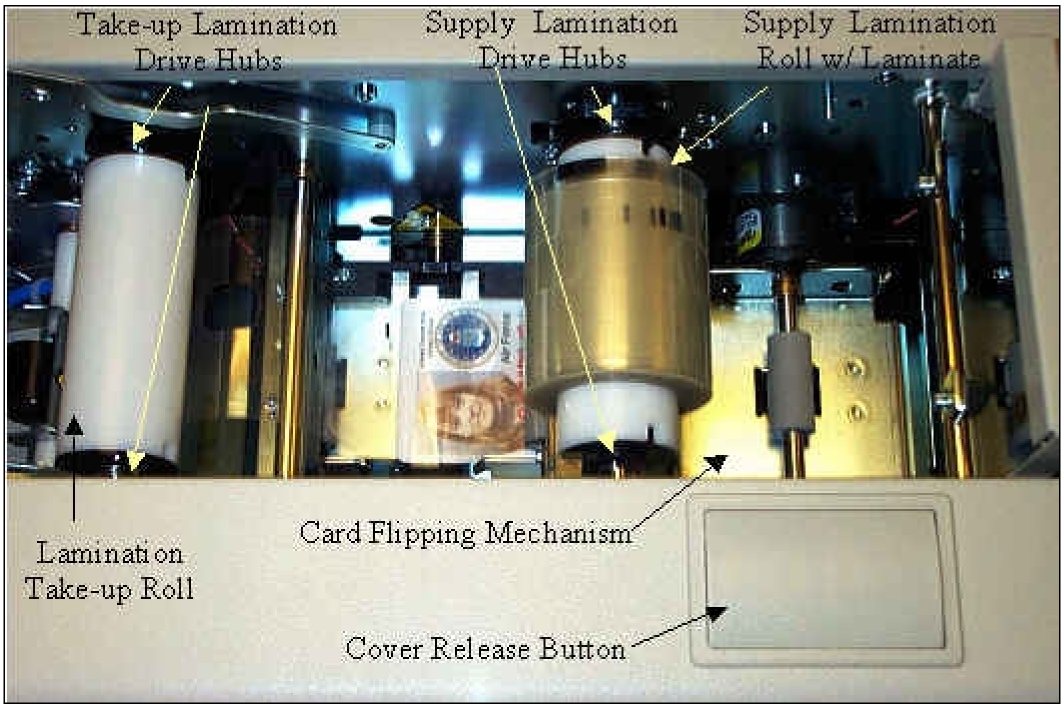


Figure 1: Printer Open Showing Card Stuck Under Laminate Roll

3. To unjam the laminate, steadily pull the laminate free from where it is jammed. If stuck to a card, pull or cut the laminate off of the card. If it is jammed underneath the rollers, press and hold down the printer's Pause/Resume button as you gently pull up on the laminate. Do not jerk the laminate to free it, since this will increase the chance of breaking it.

NOTE: If the printer laminate does happen to break, simply tape the broken end of the Supply Lamination Roll directly onto the Lamination Take-up Roll. Then, wind a few inches worth of laminate from the Supply Lamination Roll onto the Lamination Take-up Roll. Be sure the laminate is passing beneath both the supply and take-up rolls.

4. To unjam the card if it is still stuck in the printer, use the On/Cancel and Pause/Resume buttons to manually eject the card. The card that jammed should be returned through normal procedures. **NOTE**: You may need to remove the printer's color ribbon to free the jammed card.

5. Refer to the following steps, Figure 1 above, and Figures 2 and 3 below, to load the new laminate rolls into the printer.

CAUTION! DO NOT TOUCH THE METAL LAMINATION SHIELD OR THE LAMINATION ROLLER WHEN LOADING OVERLAMINATE. YOU WILL BURN YOURSELF!

a. Remove the laminate rolls from its packaging.

b. The Supply Lamination Roll is the roll containing the fresh, unused portion of laminate. The Lamination Take-Up Roll is the other one.

c. Place the Supply Lamination Roll of the laminate between the two black Supply Lamination Drive Hubs located just to the left of the printer's Card Flipping Mechanism. Make certain that the laminate material is fed from **underneath** the two rolls.

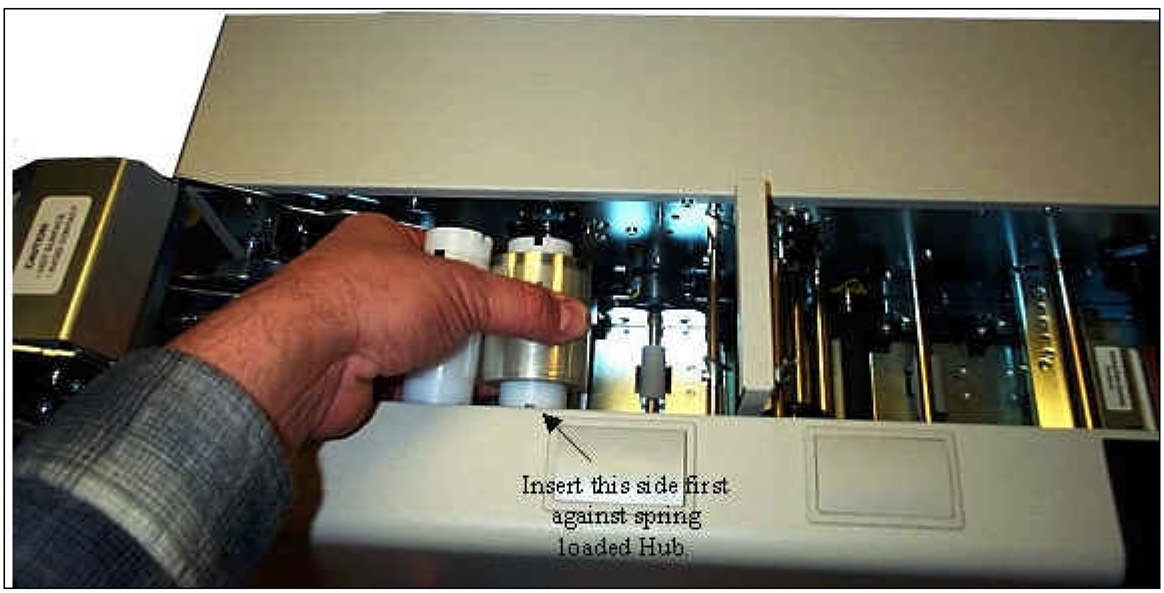


Figure 2: Inserting Supply Lamination Roll

HINT: The Lamination Drive Hubs nearest you, as you are looking into the printer from the front, are spring-loaded. Use the end of the Supply Lamination Roll to push in this hub when inserting it.

d. Place the Lamination Take-up Roll between the two black Take-up Lamination Drive Hubs located on the far left-hand side of the printer's interior. Load the take-up end of the roll just as you loaded the supply end in step 2c, above. When loaded properly, the laminate material should feed underneath both ends of the laminate rolls.

Figure 3: Inserting Lamination Take-up Roll

e. When you start to print, the Lamination Drive Hubs will automatically engage the laminate roll notches.

IMPORTANT! Do not reverse the laminate rolls. Damage may occur to the lamination roller!

6. Close the Top Covers, and press the On/Cancel button. At this point, the LCD Display will prompt you to either press the Pause/Resume button or the On/Cancel button.

   a. Pressing the Pause/Resume button will cause the printer to feed in a new card and reprint the card that originally jammed.
   b. Pressing the On/Cancel button will reboot the printer and cancel the card from the printer's memory. In this case, you must reprint the card from the RAPIDS application.

Appendix K – 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 L – Common Access Card and Consumables Order Form

Common Access Card (CAC) Stock and Consumables Order Form

INSTRUCTIONS: CAC stock and related consumables are carefully controlled and accounted for items. As such, stockpiling of CAC stock and related consumables is not permitted. To replenish your supplies, please fill out each section and follow the ordering instructions below. Address must be acceptable for receipt of registered mail. Post Office boxes are not acceptable. Annotate APO/FPO and country code if ordering from OCONUS.

Section I – Site Information

Site Name:		DEERS Site ID:	
POC Name:		Rank/Title:	/ Title
POC Email:		Comm Phone:	(###) ###-####
DSN Phone:	###-####	FAX:	(###) ###-####

Section II – Mailing Address

Attn. Line:	
Address Line 1:	
Address Line 2:	
City:	St: APO/FPO/ZIP: - Co:

Section III – Order Request

When ordering CAC stock and related consumables, generate a RAPIDS ID card report to accurately measure CAC production levels over the past 90 days. Estimate future CAC stock and consumable needs from past production as accurately as possible for the next 90-day period. Document your supply requests in the Site Remarks block and include reasoning and justification for restock requests. Due to the strict accountability of all CAC stock, each order must be evaluated prior to fulfillment. Damaged/Failed/Collected CACs must be returned before resupply. Stockpiling of CAC stock and consumables is prohibited. Note: printer ribbons and laminate have a shelf life of 12 – 18 months.

CACs produced in past 90 day period:		CAC consumables on hand:	CAC Stock: Ribbons/Laminate:

Common Access Card Stock and Related Consumable Requests

CAC Stock Request (100 per box):		Laminate rolls requested (125 per roll):	
Printer ribbons requested (250 per roll):		☐ Printer cleaning kit (Approx. one (1) every 50 Printer ribbons)	

Site Remarks:

Section IV – Ordering Information

EMAIL or FAX to your appropriate RAPIDS Support Center as listed below.

For sites in CONUS, Alaska, Hawaii, and the Caribbean	For sites in Europe	For sites in the Western Pacific
E-Mail: [illegible]	E-mail: [illegible] Copy to: [illegible]	E-mail: [illegible] Copy to: [illegible]
Commercial Fax: (703) 578-5191 Telephone: (800) 9-RAPIDS DSN: 761-8959	DSN Fax: 438-7872 Commercial Fax: 149-6971-38-7872 Telephone: 149-6971-38-7985 DSN: 438-7985	DSN Fax: 724-8204 Commercial Fax: 011-82-2-795-1092 Telephone: 011-82-2-7914-8195 DSN: 724-8195

Basic Instructions

The Common Access Card (CAC) Return Form is to be completed for each CAC that is recovered by your site. This includes any card that did not print or encode correctly, any card that is damaged or found defective, and any card that is recovered as a result of a status or rank change. This form must accompany each CAC recovered by your site, including CACs produced at other ID card activities but returned to your site, and be mailed via Federal Express to the address below once collected. Please note that this procedure does not pertain to standard teslin ID cards.

Mailing Frequency

Because CAC issue volume varies from site to site, mail all recovered CACs when you have collected 20 cards or after a 30-day period, whichever comes first. We recommend that you develop a system for storing and sending your site's recovered CACs as accountability and research into card performance in the field is crucial in the first few years of CAC implementation. Additionally, as the cost of each card is high, we intend to recover funds for each factory defective card that is delivered to your site.

IMPORTANT: All CAC stock is inventoried. Replacement card stock will be issued based on inventory records of cards issued and cards returned. Return all defective cards to DEERS. Never throw card stock away. Do not cut or mutilate recovered CACs as testing on defective cards must be performed. There is 100% accountability for all CACs.

Using the Common Access Card (CAC) Return Form

The distribution of the CAC Return Form as an electronic PDF (portable document format) allows the Verifying Official to complete and print this form on a RAPIDS workstation. After successfully logging on to RAPIDS 6.0, open the form using Adobe Acrobat Reader 3.0 or newer. Minimize the form and keep the form minimized while performing VO functions. When a CAC is turned in for reissue, returned because of a failure or defect or when an unserviceable CAC has been produced (printing, lamination or chip encoding problem) at the site, follow the following procedures for recovering a CAC:

<u>CAC Reissue (non-CAC failure)</u>

1. Open the PDF form and fill out Section One (Site Information) and Section Two (CAC Return Details).
2. Do not fill in Section 3 (Card Holder Section).
3. Scroll to the bottom of the form and select Print.
4. Recover and store the CAC and completed form.
5. Reissue a CAC, as required.
6. Click the Reset Form button.

<u>Failed CAC Return</u>

1. Open the PDF form and fill out Section One (Site Information)
2. Visually inspect the card and query the cardholder as to the failure. Annotate the CAC failure information in Section Two (CAC Return Details) including time of failure.

3. Either print the form for the cardholder to complete or survey the cardholder verbally regarding card usage and the circumstances of the failure.
4. Recover and store the CAC and completed form.
5. Reissue a CAC, as required.
6. Click the Reset Form button.

Failed CAC Production

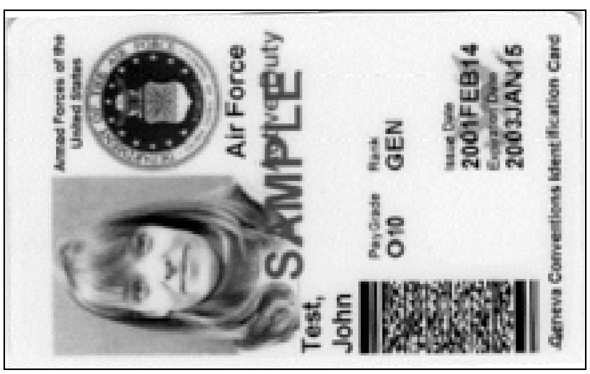
1. Open the PDF form and fill out Section One (Site Information) and Section Two (CAC Return Details).
2. Do not fill in Section 3 (Card Holder Section).
3. Scroll to the bottom of the form and select Print.
4. Store the CAC and completed form.
5. Fix know problem and reissue a CAC, as required.
6. Click the Reset Form button.

(Note: Follow guidelines for chip re-initialization if a communications problem prevented proper loading of the chip).

Form Features

The form consists of several form fields to be filled out electronically or by pen. A definition of each form field can be viewed by positioning your mouse over a gray form field. Information inputted in Section One (Site Information) will remain for each report, provided the Reset Form button is used after printing each report. Dates should be entered in the yyyyMmmdd format, as printed on the CAC. Do not attempt to affix the recovered CAC to the form. The recovered CAC number entered on the form will allow matching at a later date. Be sure to store both recovered CACs and forms in a safe area until you are prepared to mail the CACs back to DMDC for processing and accountability. The entire form will be refreshed upon closing and reopening.

Identifying the CAC Number



(Examples are not actual size.)

Each CAC is assigned a unique Identification number. This number can be found on the back of the CAC, in the upper right-hand corner, above the magnetic stripe. In this example, the number is: 2050-0000-1111-9999-8000. Please record this number on the CAC Return Form upon recovery of a CAC.

Common Access Card (CAC) Return Form

Section I

INSTRUCTIONS: Complete this form for each CAC that is recovered by your site. Mail the completed forms via FedEx, with the returned CACs, to the DEERS/RAPIDS Assistance Center (address below). Cards are to be mailed after 20 CACs have been recovered or after a 30-day period, whichever comes first. Do not cut or mutilate recovered CACs as testing on defective cards must be performed.

Site Name: ______ Site Phone: (###) ###-#### EXT ####

DEERS Site ID: ______ VO Rank/Name/Title: ______ Title

Section II

CAC Number: ####-####-####-####-#### Issue Date: yyyymmdd Recovered Date: yyyymmdd

Reason for CAC return:

- ☐ **Card Expired**
- ☐ **Card Reissue**
- ☐ **Card Failed**

Production Failure:

- ☐ **Printing**
- ☐ **Lamination**
- ☐ **Encoding**

Section III *(skip if CAC was never issued)*

Please fill out the following questionnaire regarding how you handled and used your CAC. Rate each handling section on a scale of 0 – 4, "0" being not applicable and "4" being most applicable. Circle the number that best answers the question.

CAC Handling Questionnaire:

Where is the CAC carried/kept during working hours?						**Where is the CAC carried/kept during non-working hours?**					
	0	1	2	3	4		0	1	2	3	4
	0	1	2	3	4		0	1	2	3	4
	0	1	2	3	4		0	1	2	3	4
	0	1	2	3	4		0	1	2	3	4
	0	1	2	3	4		0	1	2	3	4
	0	1	2	3	4						

CAC Use Questionnaire:

- ☐ **Visual identification only**
- ☐ **Electronic access**
- ☐ **Enter secure areas/buildings/ships**

How often per day do you use your CAC for:

CAC Failure circumstances *(if applicable)*:

Was the failure:

Was the failure associated with electronic access? ◯ Yes ◯ No

Summary of card failure:

Please provide a summary of what you were doing when first recognizing the card failure. Also include your opinion as to why the card failed (e.g. regular wear, card defect, chip related, unusual wear). Use the back of this form if additional writing space is needed.