DSL Support Documentation and FAQ

TIP: Press Control and the letter F at the same time. Type in key word(s) to search the document. Document is broken out by sections: User type, Remote Proofing, Account How-To, etc.

IMPORTANT: Close the web browser and all tabs after logging out of DSL. If the user does not close all tabs and browser, the user's PII and PHI may still be accessed due to individual computer caching. This is extremely important when sharing a computer or using a public computer

DSL frequently posts important information, tips, new requirements and other messages on the DSL home page. DSL frequently updates the Support Documentation and FAQ so it is not recommended to print this document. The document is dated in the footer

ATTENTION: MILITARY DEPENDENTS, RETIREES & THEIR DEPENDENTS:
There are other options available to you without needing to remote proof. Military Dependents, Retirees and their dependents can use their unique email registration to create their account. Make sure there is a unique email address on file for all family members PRIOR to starting the account creation process. Go to the Service Member, Retiree, and/or Military Family Members/Dependents section of this document for additional instructions

- **What is DSL?** DS Logon (DSL) is a single sign-on web application that makes it easy for the users to access their information across DoD and VA partner websites. Users have visibility to see personally identifiable information (PII); Personal Health Information (PHI); claim statuses, and records

- **Who is Eligible for an Account?** Per DoD Policy (DoDM 1341.02 vol 1), a user must be 18 years old and be affiliated with the DoD or VA, and listed in the Defense Enrollment Eligibility Reporting System (DEERS) as a Service Members (Active, Guard, Reservist, Retirees), Veterans, Dependent (e.g., spouse, ex-spouse, surviving spouse, and/or adult child receiving DoD Benefits), DoD Civilians, and Contractors

- **How DSL validates a user's identity?** DSL validates a user's identity by allowing a user to use their CAC, email registration, remote-proof or in-person proof. Email Registration is the ability to use your unique email address on file and PII to register for a DSL account. **In-person proofing** requires a user to bring I-9 documents to a Veteran Affairs Regional Office or RAPIDS office only when issuing a new ID. **Remote proofing** is a multiple step process with various workflows to validate a person's identity

- **What is the URL for DSL?** https://www.dmdc.osd.mil/identitymanagement/
  DO NOT use any URL starting with webct2. That is NOT DSL

Creating a New DSL account by User Type

Service Members:

- **USE THIS METHOD FIRST → Using a CAC** – Log into DSL. Next to your name, select "Register for a DS Logon Account" and follow the steps within the application

- **Email Registration** - Select "Create New Account" button then select "I have my DoD ID Card or CAC but no access to a card reader" and follow the steps within the application. All users must have a unique email address on their DEERS record. A user will receive a letter within 15 business days and follow the steps within the letter by going to the "Activate Account" button. Do NOT click "Create New Account" button. If users do not receive the email, check the junk/spam folder

- **RAPIDS** - While getting a new ID card, a user can notify the Verifying Official (VO) that a DSL account is wanted. The user will need to provide the VO their unique email address and follow the steps the RAPIDS Operator provides. RAPIDS site locations can be found here https://idco.dmdc.osd.mil/idco. The user will receive an email with the activation steps within 24 hours. This email is only good for 7 days

- **Dual Sponsors**: In order to view dependents, the sponsor who is receiving the benefits must go to manage relations, give permission to the spouse, and a DSL account needs to be created for the spouse

Retirees and their Dependents:

- **USE THIS METHOD FIRST → Email Registration** - Select "Create New Account" button then select "I have my DoD ID Card or CAC but no access to a card reader" and follow the steps within the application. All users, including family, must have a unique email address on their DEERS record. Unique means no other family member has the same email address. Retirees email address may be out-of-date so ensure your email address is accurate on your DEERS record prior to starting this step. A user will receive an activation email within 24 hours and follow the steps within the email by going to the "Activate Account" button. Do NOT click "Create New Account" button

- **RAPIDS** - While getting a new ID card, a user can notify the Verifying Official (VO) that a DSL account is wanted. The user will need to provide the VO their email address and follow the steps the RAPIDS Operator provides. RAPIDS site locations can be found here https://idco.dmdc.osd.mil/idco. The user will receive an email with the activation steps within 24 hours. This email is only good for 7 days. This option can only be used when a card is being issued

- **Remote Proofing** – Do not remote proof unless email registration or card issuance at RAPIDS is unavailable. If you have to remote proof for some unknown reason, DO NOT USE your Retiree or military dependent card for the documentation upload. All documents must be U.S. issued and cannot be expired. Remote proofing should be your last option. Users will need to register for a DSL by selecting "Create New Account" and follow the DSL registration procedures. Review the Remote Proofing Procedures PRIOR to starting. Registration can take up to 10 minutes

- **Dual Sponsors**: In order to view dependents, the sponsor who is receiving the benefits must go to manage relations, give permission to the spouse, and a DSL account needs to be created for the spouse.

Veterans:

- Veterans, their family members and/or dependents have the option to contact the Department of Veterans Affairs (VA) through Ask VA at https://ask.va.gov/ to work through the process of having their identity vetted and added to DEERS, if needed

- **Remote Proofing** – Users will need to register for a DSL by selecting "Create New Account" and follow the DSL registration procedures. Review the Remote Proofing Procedures PRIOR to starting. Registration can take up to 10 minutes

- Users experiencing any issues with the other credentials on VA web sites, DMDC's CCC will not be able to assist the user with any other credential. The user will need to contact the VA and/or the credential helpdesk that was used. Ask VA https://ask.va.gov/ can be used for further assistance

Military Family Member/Dependents:

- **USE THIS METHOD FIRST → Email Registration** - Select "Create New Account" button then select "I have my DoD ID Card or CAC but NO access to a card reader" and follow the steps within the application. All users must have a unique email address on their DEERS record. Family members must have unique email addresses on file. Unique means no other family member has the same email address. A user will receive an activation email with 24 hours or a letter within 15 business days and follow the steps within the letter by going to the "Activate Account" button. Do NOT click "Create New Account" button. If users do not receive the email, check the junk/spam folder

- **Remote Proofing** - Do not remote proof unless spouse is unavailable or email registration is unavailable. If you have to remote proof for some unknown reason, DO NOT USE your military dependent card for the documentation upload. All documents must be U.S. issued and cannot be expired. Remote proofing should be your last option. Users will need to register for a DSL by selecting "Create New Account" and follow the DSL registration procedures. Review the Remote Proofing PRIOR to starting. Registration can take up to 10 minutes

- **RAPIDS** - While getting a new ID card, a user can notify the Verifying Official (VO) that a DSL account is wanted. The user will need to provide the VO their email address and follow the steps the RAPIDS Operator provides. RAPIDS site locations can be found here https://idco.dmdc.osd.mil/idco. The user will receive an email with the activation steps within 24 hours. This email is only good for 7 days

- **Sponsor Request** - The Military Sponsor logs into DSL using their CAC to request an account by going to the Relationships column, select Register DS Logon for my Dependents and selecting the dependent that needs a DSL account. An activation code will be snail mailed within 15 business days and follow the steps within the letter by going to the "Activate Account" button. Do NOT click "Create New Account" button. Once this option has been selected, the spouse must wait for the activation code or 20 days before trying another method

- If the user has more than 1 sponsor, the user can select the preferred sponsor by changing the sponsors and the associated benefits with that sponsor

- **PLEASE READ IMPORTANT INFORMATION:** Sponsors can see their information and any spouse or dependent's information. For example, wife is an Active Duty Service Members, who is the sponsor. Husband is the dependent along with the couple's 3 children. Depending on the partner application a user accesses, the wife (sponsor) can view the husband's full medical records along with the children's

- **IN-PERSON PROOFING –**
  - A user can be in-person proofed ONLY when a DoD card is being issued. A user will need to make an appointment and go to a RAPIDS station and bring two I-9 documents. Acceptable I-9 documents that may be requested are:
    - Primary: Picture ID issued from Federal or State Government (e.g., valid Passport, ID card, Military Dependent card, DoD ID card, Permanent Resident Card, State DMV issued ID card, etc.)
    - Secondary: SSN card, non-picture ID card, birth certificate, citizenship or naturalization certificate, driver's license, ID card by local government with DOB, gender, height, eye color, and address
    - Your documents cannot be expired

- **REMOTE PROOFING – *READ ALL THIS SECTION PRIOR TO BEGINNING:***
  - DSL has implemented the required policies, procedures and regulations from the NIST 800-63-3 that provides instruction and standards for remote verification of an individual's identity to an identity assurance level 2 (IAL2). Remote proofing process consists of multiple workflows (documented below) that involves successfully uploading specific documentation, selfie, entering digits of a credit card/loan, and/or answering knowledge based questions. All information sent to the data vendor is encrypted and protected
  - The information used in remote proofing is pulled using a soft inquiry on a user's credit report and is not used for any other purpose except to verify the identity at a single point in time. The data, identity documents, and information provided are not used in data mining or for any other purpose except identity verification
  - If the user has reported identity theft OR the credit report is frozen, the user will need to temporarily unfreeze their credit report in order to remote proof. After proofing has completed successfully, the user is encouraged to re-add the credit freeze
  - After the user has given their consent to identity proofing, the user is required to verify their current U.S. domestic address or APO/FPO. This address must be on the user's DEERs record and reported to the credit agencies
  - The user **MUST** complete all the steps at a single time in the time limit provided. If the process is not complete, timeout occurred, or the information cannot be verified, the user's ability to access DSL and partner sites may be impacted
  - The total time should take approximately 10 minutes. Please have driver license, computer with a web camera or cell phone with a camera, a phone associated with the phone number on the user's DEERs record to receive a one-time PIN, accepted credit cards, and/or loan documents available **BEFORE** the process is started. Refer to Financial Account Information below
  - If the user is receiving an i2 error, the ability to remote proof has been suspended for 31 days. If the user tries before the 31 days, the lock-out starts over again. DMDC Customer Call Center (CCC), VA, and DSL cannot remove the lock-out as it occurs at the data vendor site

- **TWO-FACTOR AUTHENICATION (2FA)**
  - A one-time PIN (OTP) will be provided via a text or voice line that is stored in DEERS. After receiving the OTP, enter the 5-digit code into DSL
  - The code expires in 5 minutes. If the code expires or is invalid, a new code can be requested. A user has 2 attempts to enter the OTP correctly or a lock-out out for 1 hour will occur. Message and data rates may apply. DMDC Customer Call Center (CCC), VA, and DSL cannot remove the lock-out

- **MULTI-FACTOR AUTHENTICATION (MFA)**
  - A user has the option to set-up MFA using an authenticator app (e.g., Authy or Microsoft Authenticator), which must be downloaded. Cookies must be enabled on the device and follow the instructions for set-up
  - NOTE: A user must press 'SKIP' each time if a user does not want to set-up MFA
  - REMINDER: Once MFA has been set-up, this security feature can only be removed by the user or if the user no longer has the device, the user will need to contact the CCC to request MFA to be removed

- **KNOWLEDGE BASED QUESTIONS**
  - Users may be prompted to answer multiple choice questions within 3 minutes regarding their background or information that only the user may know
  - The data vendor knows the answers to the questions being asked. If the data vendor is able to verify answers are correct, the user will successfully pass this step

- **FINANCIAL ACCOUNT INFORMATION**
  - Users may be prompted to select and enter part of a credit card number or the entire loan account number for verification of a credit card or loan in their name. Credit card expiration date and security code are NOT required and there is NO hold or charge placed on the credit card. This is for identity verification only
  - The data vendor knows the answers to the questions being asked. If the data vendor is able to verify answers are correct, the user will successfully pass this step
  - The <u>following cards are **NOT accepted**</u> because the data vendor cannot verify the account: American Express, Debit, Barclays, Kohls, Utility, Cash Back, Student, Balance Transfer, and Travel Rewards Cards
  - The credit card cannot be in dispute, suppressed, frozen or expired, and must be in the user's name and on the user's credit report

- **DOCUMENT UPLOAD**
  - Users may be prompted to upload a U.S. identity verification document and take a selfie. (A selfie is a picture of one's full face with nothing else in it or beside it) and by following the instructions. The following documents **<u>cannot be uploaded</u>** for verification: Military ID, Veteran/DAV, PIV, expired ID card and/or foreign issued documents
  - Users on a computer may be prompted to select an image stored on their device instead of taking a picture or seek assistance from a friend or family member when capturing documents and/or selfies
  - Images must be 'jpg' with size 480x640 or greater, 24 bit color and at least 250 dpi. If the photo takes several minutes to upload, the photo may be too large. Default settings are recommended

- **IDENTITY DOCUMENTS**: Use a solid-dark background when taking the picture of a VALID, unaltered, document. Do not place on lap, patterned couch, hold the document or cover any part of the document. Ensure there is no glare or reflection and the pictures are taken directly above and NOT at an angle. Document in photo must be sharp, clear and easy to read with no parts cut off by the photo

- **SELFIE**: Use a solid background. Do not wear hats, glasses, distractive clothing, face masks, or filters. Look straight into the camera and do not turn head sideways or take photo downward. Do not take a photo of a photo. Your face should fill most of the photo

- **EXAMPLES OF FAIL DOCUMENT SUBMISSIONS:**
  - Poor quality document or selfie photo: Not clear, blurry, emoji or fingers covering portions, hats, glasses, while driving, multiple people or animals in photo, mirror is used, hair hiding face, angle is not straight forward, document is damaged, filters are used
  - Backgrounds are bad: Multi-colored patterned couches and/or chairs, lass tables that reflect the camera flash, multi-colored carpets, bookshelves with tons of books, in front of framed photos of the family, family/friends/pets cannot be in any of the photos

- **EXAMPLES OF PASSING DOCUMENT SUBMISSIONS:**
  - Document is placed on a dark surface with good lighting, no glare, easily readable in the photo and nothing is covered up, document is U.S. issued, not expired, and not military issued
  - Selfie is full face front with no sunglasses, hats, hair, masks or anything else that would take away from seeing the full face. Think driver's license photo

- **BEST PRACTICES:**
  - Do not give username/password information to anyone. Be sure the device's software and malware/virus protection are up-to-date. Only install software from the software provider's official website. Do not click on any emailed links to install something. Be cautious of messages, links and ads on social media as those can contain viruses. When in doubt, do not click on them
  - Proactively verify accounts and data (e.g., eBenefits, bank accounts, credit reports, DSL) on a monthly basis to ensure information is still accurate
  - If a user thinks their account has been compromised or hacked, change password and challenge questions immediately, verify banking information is still accurate, and may want to freeze their credit report
  - DMDC CCC nor the DSL team will not initiate first contact with users via email or telephone to request PII or sensitive DSL account information (username, password, challenge questions). If a user thinks there is a fraudulent email, website or phone call, log into the DSL account and immediately change the password and challenge questions
  - Users must login at least once every 180 days (6 months) to keep the account active and must reset password every 60 days (2 months). Users will be prompted to change password before expiration and will be notified to sign-in prior to deactivation
  - Users are responsible for keeping their information (e.g., name, address, phone numbers, email) current on their DEERS record

After DSL account is created

- Browsers to use for optimal user experience are Chrome, Edge and Safari. Internet Explorer is no longer supported

- Users can log into DSL by using their DSL username/password, a CAC, or a PIV by selecting the appropriate tab

- PIV Login - Select PIV tab. When first logging in, the user will need to register their PIV by entering their name, date of birth, person identifier, and DSL username/password then the user can use their PIV to log into DSL. If the DSL account is deactivated, the user will need to create a new DSL account and re-register their PIV card

- **Two Factor Authentication (2FA) One Time PIN (OTP):**
  - When the user logs in, changes password and/or create a DSL account, the user will be asked to input a PIN that will be sent to their landline or text to their cell phone.
  - Once the methodology (text or phone call) is selected, the user will receive a PIN. The user will need to input the PIN into the text box provided. The user can request to resend the PIN on the screen. **NOTE:** Message and data rates may apply. If the user is using an international number, not all countries support text and/or voice authentication codes. The phone number cannot have a leading zero(s)

- **Multi Factor Authentication (MFA) One Time PIN (OTP):**
  - If the user has set-up the MFA option using a downloaded app, the user will be prompted to enter the 6-digit code from the authenticator app. If the does not want to set-up the MFA, select SKIP

- **Activation Code:**
  - After an Activation code is emailed, select "Activate Account" – Do not select Create New Account
  - If there is no unique email or no email, an incorrect address or no address, the user will need to go to IDCO (https://idco.dmdc.osd.mil/idco/) and update their contact information, update during card issuance or call the DMDC CCC

- **Challenge Questions:**
  - Challenge questions are created by the user and used to reset passwords in the event of forgotten password or account suspended due to too many incorrect password attempts. Select questions and enter answers that can remembered in the future to use to reset password
  - Avoid odd answers or multiple words. Answer questions that a user CAN remember over a long period of time. Ensure that none of the social media accounts contain the answers to the challenge questions
  - The DMDC CCC cannot create, change or remove challenge questions
  - A user can change their challenge questions and answers anytime by logging into DSL and selecting Change Challenge Questions

- **Document Upload Identity Verification:**

- If prompted to upload U.S. documents or a selfie, it is recommended using a smart device (e.g., cell phone) with access to cameras
  - The user cannot use DoD issued ID cards for remote proofing. These include the Military ID card, Dependent ID card, Veteran/DAV card, PIV card, or an expired ID card of any type
- When finishing uploading U.S. documents, click on Verification Status button after one (1) minute to monitor the status of the request
- Only .jpg images are supported when selecting an image
- Documents are only used for identity purposes and will not be stored nor used after identity verification has occurred
- When taking a photo of a document, the document cannot be a photocopy
- You cannot cover or hide any part of a document, front or back
- Military, Veteran, Foreign and expired documents CANNOT be verified by the data vendor

- **Manage Relationships:**
  - There are several available options such as people who can act on behalf of the user or people that can act on for THEIR behalf
  - **PLEASE READ IMPORTANT INFORMATION**: Sponsors can see their information and any spouse or dependent's information. For example, wife is an Active Duty Service Members, who is the sponsor. Husband is the dependent along with the couple's 3 children. Depending on the partner application a user accesses, the wife (sponsor) can view the husband's full medical records along with the children's. Clinical access authorizes full access to medical records for that individual
  - Be mindful that these authorizations remain active until the authorizing individual revokes them within the DSL application
  - The user can manage their relationships by logging into DSL, select Manage Relationships, then select Add Relationships and select option that applies
  - **Dual Sponsors**: In order to view dependents, the sponsor who is receiving the benefits must go to manage relations, give permission to the spouse, and create a DSL username/password account for the spouse. Currently, the spouse must log into DSL using the username/password and not their CAC to see the other dependent's (e.g., children) information

- **Surrogate Accounts**:
  - Surrogate accounts will only be established after an individual has been legally deemed a surrogate to a DoD Beneficiary. The individual will need to:
    - Be added to DEERS by going to local military issuing Identification (ID) card facility (RAPIDS Site Locator: https://idco.dmdc.osd.mil/idco/locator)
    - Contact the facility prior to driving to it to make an appointment and communicate that the appointment is to establish surrogacy
    - Bring two I-9 identity documents (e.g., Social Security Card, Birth Certificate, State or Federal Issued Photo ID such as a Driver's License or Passport) to the appointment. These identity documents are for the surrogate, not the DoD Beneficiary
    - Fill out the DD Form 3005 "Application for Surrogate Association for DoD Self-Service (DS) Logon" and bring the completely filled out form to the appointment. The form will need to contain all required signatures such as a certifying official

(Staff Judge Advocate (SLA), Judge Advocate General (JAG), legal representation, or Service Project Officer (SPO). If the form does not have all signatures prior to going to the facility, the form will be rejected and an account cannot be issued
    - Bring all supporting court documentation (e.g., power of attorney, etc.) to the appointment
  - After the surrogate identity is added to DEERS, an email or a letter via the US Post Office will be sent to the surrogate that contains instructions on how to activate the DSL surrogate's account
  - The surrogate's account will remain active as long as DoD Beneficiary remains eligible for a DSL account. Once the DoD Beneficiary is no longer eligible for a DSL account, the surrogate's account will automatically be deactivated

- **Account Suspended**
  - When a DSL account is suspended, the user will need to log into DSL and select Un-suspend My Account or select Forgot Password? The user will need to answer the challenge questions correctly then will be prompted to change their password

- **Password Information**
  - The user can change their password at any time, but it MUST be changed at least every 60 days (2-months). To change a password, the user will need to log into DSL and go to manage DSL account then select Change Password
  - If the user forgot their password, the user will need to go to DSL and select Forgot Password? and follow the instructions on the remaining steps
  - **Passwords must:**
    - be between 15 and 128 characters in length
    - contain at least 1 uppercase letter (A-Z)
    - contain at least 1 lowercase letter (a-z)
    - contain at least 1 number (0-9)
    - contain at least 1special character (i.e. @_#!&$'%*+().,;~:{}|?>=<^[]-)
    - contain at least 8 characters that are different from the previous passwords
  - **Passwords cannot:**
    - have spaces
    - be 1 of the last 10 previous passwords
    - have users birthdate, SSN, name, phone number, or ZIP Code
    - have been changed within the last 24 hours

- **Adding, Updating, or Correcting Data Records**
  - Using the DSL account or CAC, the user can update their address, email address and/or phone number(s) by logging into DSL and selecting Update Contact Information
  - Go to IDCO to update address, email address and/or phone number by logging into IDCO (https://idco.dmdc.osd.mil/idco/), under "My Profile" and select "Continue". The user will go to the bottom of the screen after updating the information and click "Submit"
  - If the above options do not work, the user can contact the DMDC CCC to update their information. Dependents over 18 must update their own information. Documents may be requested to be submitted via mail or fax
  - In-person updates, the user can call to make an appointment at a RAPIDS station and

bring in I-9 documents to verify their identity

- **Account Locks, Deactivations, & Suspensions**
  - A user can deactivate their account at any time. An account can be re-established at any time by registering for a new account and completing the identity verification process
  - DSL accounts can be locked for a variety of reasons to include unusual activity and cannot be unlocked by the user. Account locks can only be unlocked by DMDC. Account locks are not the same as account suspended or an account that has been deactivated. If the account is locked, the user can contact the DMDC CCC to see what options are available to request the account be unlocked
  - An account can be suspended due to incorrect password attempts
  - Accounts will be deactivated due to inactivity in 180 days (6 months)
  - If the user has unsuccessfully tried to remote proof multiple times and now receiving an i2 error, the user's ability to remote proof has been suspended for 31 days. If the user tries again, the 31 day timeline will start over again. DMDC CCC, VA, and DSL cannot remove the suspension to remote proof as it occurs as the data vendor site

Error codes

- **Error Code [3]** – A username and password is required when logging into DS Logon. Enter your username and password. If you do not remember your username/password, go to Forgot username or Forgot password.

- **Error Code [4]** - The DS Logon password is required. You did not enter password when attempting to log on. Fill out all required items when logging in. This includes username and password.

- **Error Code [5]** - If you do not remember your username/password, go to Forgot Username or Forgot Password. If you do not have an account, go to "Create Account".

- **Error Code [7]** - Your request for an account is being processed. You will receive an activation letter to your mailing address. Once you have received, follow the instructions on the letter.

- **Error Code [8]** - Your account has been suspended due to excessive failed logon attempts. Go to Unsuspend Your Account if you still need to access your account.

- **Error Code [9]** - This account is locked. Go to the FAQs for what actions are available to you.

- **Error Code [10]** - The DS Logon username or password you entered is INVALID. Do you need to register for a DS Logon?

- **Error Code [11]** - The DS Logon username or password you entered is incorrect. Use Forgot Username or Forgot Password for recovery methods or if you do not have an account, register for one.

- **Error Code [12]** - Your password needs to be reset. Go to Forgot Password to reset your password.

- **Error Code [13]** - You are not eligible for a DS Logon Account. If you are a Veteran or believe you are eligible for an account, visit the simplified FAQs for what actions are available to you to get a DS Logon account.

- **Error Code [14]** - The one-time password has expired. You will need to restart the logon process to be able to log into DS Logon.

- **Error Code [31]** - Unable to read your Common Access Card (CAC). Try again after ensuring your CAC is valid, fits tightly in your smart card reader, and the reader is connected to your machine.

- **Error Code [32]** - There was a problem reading your Common Access Card (CAC). Make sure your CAC is valid, fits tightly in your smart card reader, and the reader is connected to your machine.

- **Error Code [33]** - DS Logon is unavailable. Try again later or you can visit the simplified FAQs for further options.

- **Error Code [34]** - There was a problem reading your Common Access Card (CAC). Make sure your CAC is valid, fits tightly in your smart card reader, and the reader is connected to your machine.

- **Error Code [35]** - There was a problem reading your Common Access Card (CAC). Make sure your CAC is valid, fits tightly in your smart card reader, and the reader is connected to your machine.

- **Error Code [36]** - There was a problem reading your Common Access Card (CAC). Make sure your CAC is valid, fits tightly in your smart card reader, and the reader is connected to your machine.

- **Error Code [37]** - The system is unavailable. Try again later. If this problem continues you may contact the DMDC Support Center (DSC) at 800-477-8227. To best assist you, call when you are at a computer if possible.

- **Error Code [38]** - There is an issue with your CAC. It may be invalid, revoked, expired or an issue with the certificates. If you believe you have received this message in error, call the DMDC Customer Contact Center at 800-368-3665 for further assistance.

- **Error Code [39]** - Your digital certificate on your Common Access Card (CAC) is not unique in our system. If you believe you have received this message in error you may contact the DMDC Customer Contact Center at 800-368-3665 for further assistance. To best assist you, call when you are at a computer if possible.

- **Error Code [40]** - There was a problem with your digital certificate on your Common Access Card (CAC). If you believe you have received this message in error you may the DMDC Customer Contact Center at 800-368-3665 for further assistance. To best assist you, call when you are at a computer if possible.

- **Error Code [41]** - The system is unavailable. Try again later. If this problem continues you may contact the DMDC Support Center (DSC) at 800-477-8227. To best assist you, call when you are at a computer if possible.

- **Error Code [42]** - The information you provided was not found or there may be an error on the record in Defense Enrollment Eligibility Reporting System (DEERS). Ensure you are using your legal first and last name. If you are using your legal name or your name has changed, go to the simplified FAQs for what actions a user must take to update their information or you can contact the DMDC Customer Contact Center at 800-368-3665 for assistance.

- **Error Code [43]** - We are unable to locate your record based on the information you entered. If this continues contact the DMDC Customer Contact Center at 800-368-3665 for further assistance. To best assist you, call when you are at a computer if possible.

- **Error Code [44]** - We are unable to locate your record based on the information you entered. Try again. If this continues contact the DMDC Customer Contact Center at 800-368-3665 for further assistance. To best assist you, call when you are at a computer if possible.

- **Error Code [45]** - We are unable to locate your record based on the information you entered. Try again. If this continues contact the DMDC Customer Contact Center at 800-368-3665 for further assistance. To best assist you, call when you are at a computer if possible.

- **Error Code [46]** - The system is currently unavailable. Try again later. If this problem continues, you may contact the DMDC Support Center (DSC) at 800-477-8227 for assistance. To best assist you, call when you are at a computer if possible.

- **Error Code [47]** or **[49]** - The system is currently unavailable. Try again later. If this problem continues, you may contact the DMDC Support Center (DSC) at 800-477-8227 for assistance. To best assist you, call when you are at a computer if possible.

- **Error Code [50]** - We have located your Defense Enrollment Eligibility Reporting System (DEERS) record; however, it appears there may be invalid information on file. You may contact the DMDC Customer Contact Center at 800-368-3665 for assistance. To best assist you, call when you are at a computer if possible.

- **Error Code [53]** - Your Common Access Card (CAC) certificates are invalid and access is revoked. If you believe you have received this message in error you may contact the DMDC Customer Contact Center at 800-368-3665. To best assist you, call when you are at a computer if possible.

- **Error Code [54]** - Your Common Access Card (CAC) is expired and access is revoked. Visit your nearest ID card facility to obtain a new card. You can locate the nearest ID facility at RAPIDS Site Locator.

- **Error Code [55]** - Your Common Access Card (CAC) is reported as lost and access is revoked. Visit your nearest ID card facility for assistance with obtaining a new card. You can locate the nearest ID facility at RAPIDS Site Locator.

- **Error Code [56]** - Your Common Access Card (CAC) is terminated and access is revoked. Visit your nearest ID card facility to obtain a new card. You can locate the nearest ID facility at RAPIDS Site Locator.

- **Error Code [57]** - The system is currently unavailable due to an outage within another internal system. We hope to have the issue resolved soon, so try again in a few hours. If this problem continues after that time period, you may contact the DMDC Support Center (DSC) at 800-477-8227 for assistance. To best assist you, call when you are at a computer if possible, and be prepared to provide your Personal Identifiable Information if asked to research your specific record.

- **Error Code [61]** – We couldn't access your DEERS record, possibly due to a data error on your record. Try again later. If this problem continues, you may contact the DMDC Customer Contact Center (CCC) at 800-368-3665 for assistance. To best assist you, call when you are at a computer if possible, and be prepared to provide your Personal Identifiable Information if asked to research your specific record.

- **Error Code [62]** - Your CAC has been identified as having excessive access which has been flagged as potential fraudulent access. In order to protect your PII and PHI, please contact the DMDC Customer Contact Center (CCC) at (800)-368-3665 to go through their identity verification process which includes submitting state or federal issued identity documents.

- **Error Code [63] -** There was a problem reading your PIV. Make sure your PIV is valid, fits tightly in your smart card reader, and the reader is connected to your machine.

- **Error Code [64]** - You do not have a DS Logon account. Select 'Create Account' and complete registration.

- **Error Code [65]** - You do not have an active DS Logon account. Select 'Create New Account' and complete registration.

- **Error Code [66]** - Your PIV is not registered. You will now be redirected to complete your PIV registration.

- **Error Code [67] -** Your PIV cannot be registered with the current DS Logon credential.

- **Error Code [68] -** Select the CAC tab to login using your CAC.

- **Person Error Code [p1]** - The personal information you provided was not found in Defense Enrollment Eligibility Reporting System (DEERS). Try again.
  Ensure that you enter your personal information accurately, using your legal first and last name. If your name has changed since you or your sponsor served, contact the DMDC Customer Contact Center (CCC) at 800-368-3665 for assistance with changing your name in DEERS. Veterans (and their family members/dependents) may contact the Department of Veterans Affairs (VA) to have your identity validated and added to DEERS. You may also call the VA at 800-827-1000 for assistance directly, and say "eBenefits" when you are prompted for the reason for your call. You are responsible for keeping your information current in your DEERS record. You must take action to register your family members/dependents and ensure they are correctly entered into DEERS. Once registered in DEERS it is important to keep your DEERS records updated when personal eligibility information changes. This includes contact information and family member status (marriage, divorce, birth, adoption, etc.).

- **Person Error Code [p2]** or **[p3]** or **[p10]** - We have located your Defense Enrollment Eligibility Reporting System (DEERS) record; however, it appears there may be invalid information on file. You may contact the DMDC Customer Contact Center at 800-368-3665 for assistance. To best assist you, call when you are at a computer if possible.

- **Person Error Code [p4]** or **[p5]** - The personal information you provided was not found in Defense Enrollment Eligibility Reporting System (DEERS). Try again. If this problem persists, you may contact the DMDC Customer Contact Center at 800-368-3665 for assistance. To best assist you, call when you are at a computer if possible.

- **Person Error Code [p6]** - Based on the information you provided, your Defense Enrollment Eligibility Reporting System (DEERS) record reflects that you are ineligible to obtain a DS Logon. Veterans (and their family members/dependents) may contact the Department of Veterans Affairs (VA) to have your identity validated and added to DEERS. You may also call the VA at 800-827-1000 for assistance directly, and say "eBenefits" when you are prompted for the reason for your call.

- **Person Error Code [p7]** or **[p8]** or **[p9]** - The personal information you entered does not match the information found in Defense Enrollment Eligibility Reporting System (DEERS). If this problem persists, you may call the DMDC Customer Contact Center at 800-368-3665 for assistance. If you are enrolled in DEERS but your name has changed since you served, contact the DMDC Customer Contact Center at 800-368-3665 for assistance with changing your name in DEERS. To best assist you, call when you are at a computer if possible.

- **Identity Proofing Error Code [i1]** - We are unable to remotely verify your identity. See the FAQs for alternative methods for identity verification.

- **Identity Proofing Error Code [i2]** - You have reached the maximum number of attempts to remote proof your identity. You will need to in-person proof to verify your identity

- **Identity Proofing Error Code [i3]** - DSL is unable to verify your identity remotely. Please use other options (e.g., in-person) to complete the verification process.

- **Identity Proofing Error Code [i4]** - At this time, we are unable to remotely proof your identity. Pursue our In-Person identity proofing options to verify your identity.

- **Identity Proofing Error Code [i5]** - The time limit for the remote proofing has expired. You can try again or visit the FAQs for alternative methods for identity verification.

- **Identity Proofing Error Code [i6]** - The remote proofing service is unavailable. You can wait and try again or visit the FAQs for alternative methods for identity verification.

- **Identity Proofing Error Code [i7]** - We are unable to remotely proof your identity. Pursue our In-Person identity proofing options to verify your identity.

- **Identity Proofing Error Code [i8]** - You are only allowed one session at a time to remote proof your identity. Close all your windows and try again.

- **Identity Proofing Error Code [i9]** - DS Logon is unavailable. Try again later or you can visit the simplified FAQs for further options.

- **Identity Proofing Error Code [i10]** – At this time, we are unable to remotely proof your identity. (Note: this is due to there not being enough credit history on file to verify your credit history. You will not be able to proof your identity online)

- **Identity Proofing Error Code [i11]** - We are unable to continue to remote proof your identity at this time. If you are initially logging in, please try a different device (e.g., computer, tablet, phone). If you are in the middle of remote proofing your identity, please refer to our FAQs for an alternative option.

- **Identity Proofing Error Code [i12]** - You have reached the maximum number of attempts to remote proof your identity and cannot remote proof again for 31 days. The DMDC Customer Call Center (CCC) cannot re-establish the capability to remote proof again prior to the 31 days. For additional information or alternative options, read DSL Support Documentation/FAQ located on the login screen by clicking the Need Support? button.

Contact Centers

First, **READ** the FAQs located in **Need Support?** All of the information for self-help is in the FAQs.

Organization	Contact and operation hours	Helps With
DMDC Customer Contact Center (CCC)	Phone: 800-368-3665 Hours: Mon-Fri 5am – 5pm PT	DEERS data or CAC Issues, and DSL account information. Does not help with ID.me or Login.gov

RAPIDS Site Locator	https://idco.dmdc.osd.mil/idco/	
Veteran Affairs (eBenefits)	Phone: 800-827-1000 Hours: Mon-Fri 5am – 5pm PT	Veteran adding an identity to DEERS, Benefits Questions (GI Bill, Claim Status or Disability Benefits)
Veteran Affairs (eBenefits)	Phone: 800-983-0937 Hours: Mon-Fri 5am – 5pm PT	Technical Issues, such as password changes or error codes

Other Partner Helpdesks

Organization	Contact Info
Health Net Federal Services, LLC (TRICARE West Region)	1.844.866.9378
Humana Military (TRICARE East Region)	1.800.444.5445
US Family Health Plan	1.800.748.7347
TRICARE Dental Program (UCCI)	1.844.653.4061
Active Duty Dental Program (UCCI)	1.866.984.2337
TRICARE For Life	1.866.773.0404
TRICARE Mail Order Pharmacy (Express Scripts, Inc.)	1.877.363.1303
Military Health System Help Desk	1.800.600.9332
TRICARE Retail Pharmacy (Express Scripts, Inc.)	1.877.363.1303
Federal Employees Dental and Vision (FEDVIP)	1.877.888.3337
Military Medical Support Office	1.888.647.6676