VA | U.S. Department of Veterans Affairs

US Department of Veterans Affairs
CEIAESA (EA)

Standard Operating Procedures (SOP)

Version 2.0, February 2025

Table of Contents

Section 1 | Purpose....3

Section 2 | Contract Summary....3

2.1 Contract Information....3

2.2 Contract Overview....3

2.3 Summary of Coverage....3

2.3.1 Cisco SmartNet Total Care (SNTC)....3

2.3.2 High-Touch Operations Management (HTOM)....3

2.3.3 High-Touch Technical Support (HTTS)....3

2.3.4 Cisco Certified Architects and Engineers for Enterprise-wide Solutions....4

Section 3 | Technical Assistance Center (TAC) Support....4

3.1 What's covered?....4

3.2 How to Open a TAC Case....4

3.3 Severity Level Descriptions....4

3.4 Case Escalation Procedure....5

Section 4 | Asset Management Portal....5

4.1 View My Assets....5

4.2 Submitting a Request....5

4.3 Reports....5

4.5 Gaining Access to the Portal....6

4.6 Asset update process defined....6

4.7 User Roles Defined....6

Appendix A | How to create a user ID for the Iron Bow Portal....7

Appendix B | Portal Request type defined....9

Appendix C | Abbreviations and Definitions....10

Section 1 | Purpose

This document provides the standard operating procedures for the *Department of Veterans Affairs Smartnet Enterprise Agreement*. This and many other resources are found at Iron Bow's Resource website. For any questions or concerns, please email *VAsmartnetEA@ironbow.com* for a prompt reply.

Section 2 | Contract Summary

2.1 Contract Information

Contract Name:	*VA CEIAESA*
Cisco Contract Number:	*206257319, 206257318, 206259048*
Reseller:	Iron Bow Technologies
Period of Performance (PoP):	Base: 10/1/2024 – 9/30/2025 OY1: 10/1/2025 – 9/30/2026

2.2 Contract Overview

In *October of 2024* the Department of Veteran Affairs, signed an agreement, *CEIAESA*. This contract provides the customer access to SmartNet Total Care for all Cisco devices, which provides 24x7 technical support through online and a toll-free telephone call-in service, provides next business day hardware replacement. The prime contract holder, Iron Bow Technologies, is partnered with Cisco to provide all capabilities within this contract.

2.3 Summary of Coverage

2.3.1 Cisco SmartNet Total Care (SNTC)

- Provides unlimited 24x7x365 Technical Assistance Center (TAC) online and 800 telephone service; case prioritization occurs using one of four severity levels
  - Severity 1 or 2 – Call 866-748-0639, Option 1 for immediate response
  - Severity 3 or 4 – Open a new case at https://sctp.cisco.com
- Provides 8x5xNext-Business-Day replacement for all customer-owned, Cisco-branded, hardware
- Provides unlimited Internetwork Operating System (IOS) update and patch downloads
  - Access Download from Cisco Software Central: https://software.cisco.com

2.3.2 High-Touch Operations Management (HTOM)

Cisco single point of contact for all support assistance, prioritization, and management within this contract. For questions and concerns, contact *va-htom@cisco.com.*

2.3.3 High-Touch Technical Support (HTTS)

- Personalized, high-touch support: expedited routing and call handling with limited after hours on-call support
- **Note**: Most technologies are supported from 8:00 a.m. – 8:00 p.m. (Eastern)

2.3.4 Cisco Certified Architects and Engineers for Enterprise-wide Solutions

There are *13* Cisco-certified solution architects/engineers to deliver and manage, design and strategic engineering, solutions for Department of Veteran Affairs. This team works hand-and-glove with the customer on enterprise-wide engineering solutions.

Section 3 | Technical Assistance Center (TAC) Support

3.1 What's covered?

The customer is provided unlimited 24x7x365 TAC support for all customer-owned, Cisco-branded, hardware and software and SWSS-eligible application software (owned as of 21 June 2019).

3.2 How to Open a TAC Case

TAC Cases can be opened by navigating to https://sctp.cisco.com (member must login in with their Cisco CCO ID credentials if needed see process doc here on how to create a CCO ID).

For Severity Levels 1 and 2 TAC Cases:

- Call the HTTS Frontline at 866-748-0639 so an HTTS Representative can open a case on your behalf and Transfer you to an HTTS engineer

For Severity Levels 3 and 4 TAC Cases:

- Open your service request using the online tool: (Secure Case Tracking Portal) at https://sctp.cisco.com

Information Needed to Open a Service Request:

- Your Cisco.com ID and contact information (full name)
- Severity of your service request (See para 3.3, Severity Level Descriptions.)
- Preferred contact method (email, phone number)
- Enterprise Agreement Contract# *206257319, 206257318, 206259048* and device serial number
- Description of your issue (symptoms, business impact, technology)
- Site information (for verification purposes)
- Details on troubleshooting steps you have taken.

3.3 Severity Level Descriptions

Severity 1 (S1): Network or environment is down or there is a critical impact to the requestor's mission. The requestor and Cisco will commit full-time resources to resolve the situation. Cisco is committed to restore services within 4 hours.

Severity 2 (S2): Network or environment is severely degraded. The requestor and Cisco will commit full-time resources during standard business hours to resolve the situation. Cisco is committed to restore services within 8 hours.

Severity 3 (S3): Network or environment is impaired. The requestor and Cisco commit resources during standard business hours to resolve. Cisco is committed to restoring services by the next business day.

Severity 4 (S4): Information is required on Cisco product capabilities, installation, or configuration. There is little or no impact on the requestor's mission. Cisco is committed to restoring services by the next business day.

3.4 Case Escalation Procedure

If a case is not progressing adequately or the quality of service is not satisfactory, the Requestor/Unit/Program/Agency can escalate the case with the following process:

- During normal business hours 8:00 am – 8:00pm (Eastern): Contact Cisco TAC at 1-800-553-2447 and request the TAC case have its severity level raised. The HTOM Team can also be contacted by emailing *va-htom@cisco.com*.
- After normal business hours (including weekends/holidays): Contact Cisco TAC at 1-800-553-2447 and request to raise the TAC case's severity level with the on-shift TAC Duty Manager. Outside of 8:00 a.m. – 8:00 p.m. on regular duty days, advanced support is available by engaging the on-call U.S. Public Sector HTOM by email at ggsghtom@epage.cisco.com.

Section 4 | Asset Management Portal

This portal is intended to assist the VA during the lifecycle of the Enterprise Agreement procured through Iron Bow. The portal will assist you in managing your assets, provide you with a documentation database, and ease of access to Iron Bow advanced Services. This document will show you how to navigate the portal.

4.1 View My Assets

By Selecting the "View My Assets" button, a new page will be opened to the asset list. The assets listed in this page are already added to the contract and can be viewed by clicking the serial number on the left-hand side of the table. Additionally, you can filter by any of the fields listed in this table at the top of the page by selecting the half hourglass icon. If the information listed for the asset is not correct, please see **Appendix B** on how to open a request.

4.2 Submitting a Request

The "Submit A Request" button will navigate you to a second page consisting of fields to be completed. Select what type of request you are submitting and complete the fields to the best of your knowledge. The more information provided will a result in a faster resolution from the XR team.

Request types:

- MACD Requests (Moves, Adds, Change, Delete)
- Reporting requests
- Other

4.3 Reports

The "Reports" button will populate multiple reports regarding your enterprise agreement. This is sorted by report type, year, and month. The reports will be created by the XR team and uploaded to the tool on a scheduled basis.

4.4 Resources

The "Resources" section is managed by the XR team to provide you with important documentation regarding the enterprise agreement. IE: SOP, FAQs, Quick Reference Guides, contact sheets, Recorded trainings, and Process documentation.

4.5 Gaining Access to the asset management portal

The asset management portal is a role-based system that allows the VA and Iron Bow to better manage the assets in the VAs install base. To gain access to the portal start at this page Click Here and follow the process outlined in Appendix A.

4.6 Asset update process defined

The data reflected in the tool is what is listed in the Cisco system as covered under the contract. Iron Bow works hand in hand with Cisco and the VA to ensure the data is as accurate as possible. If there is a change that needs to be made, please submit a case for a MACD request type and define what action should be take on the devices. Once a request is received in the Iron Bow system the XR team will acknowledge the request and take it to VA leadership for approval. Once approved by VA leadership the XR team will notify Cisco asset management to ensure the update is made in their end as well as the Iron Bow tool. Please note, that the XR team will keep the case as up to date as possible during this time to ensure the requestor is kept in the loop. If the change is denied by VA leadership the XR team will notify the requestor with the reason for the decision and close the case.

4.7 User Roles Defined

The VA portal has a role-based access privileges as mandated and assigned by the VA

1.) Admin: Admin users are defined as Iron Bow System admins. This role is not designed for VA use as it is a level of access reserved for the system hosts and backend support.

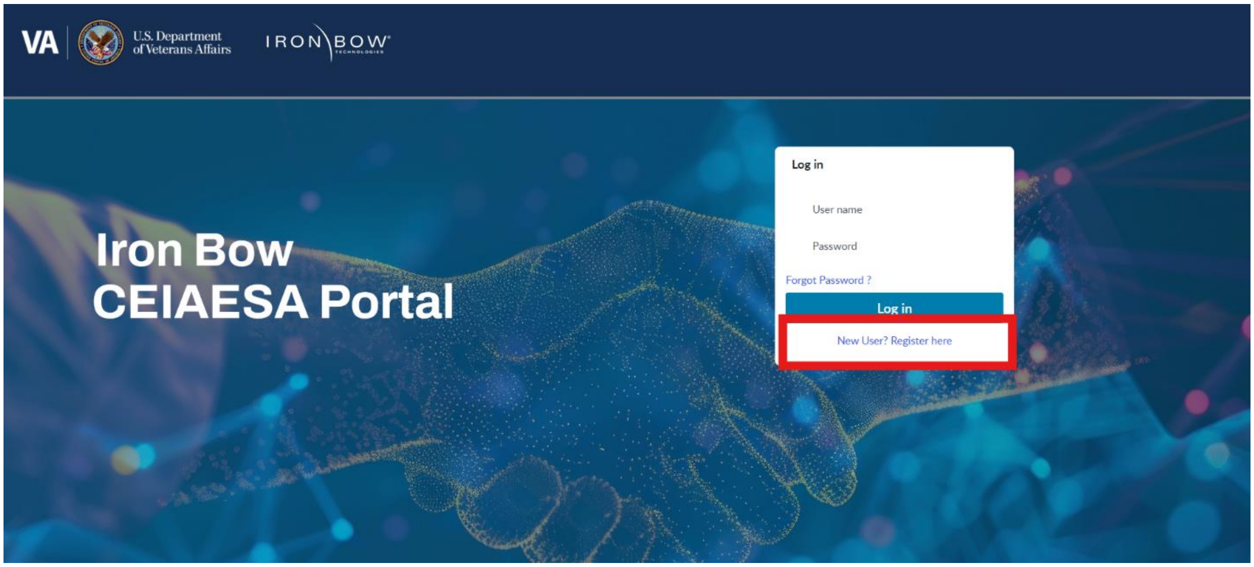
2.) Super Users: Super users are VA employees that have been designated by VA leadership to be trusted approvers of requests that come through the system from regular users. This user type has elevated privileges from the normal users to see all cases and requests in the system as well as approve new users and download the asset list.

3.) Users: Can see assets Submit requests and see ONLY their tickets.

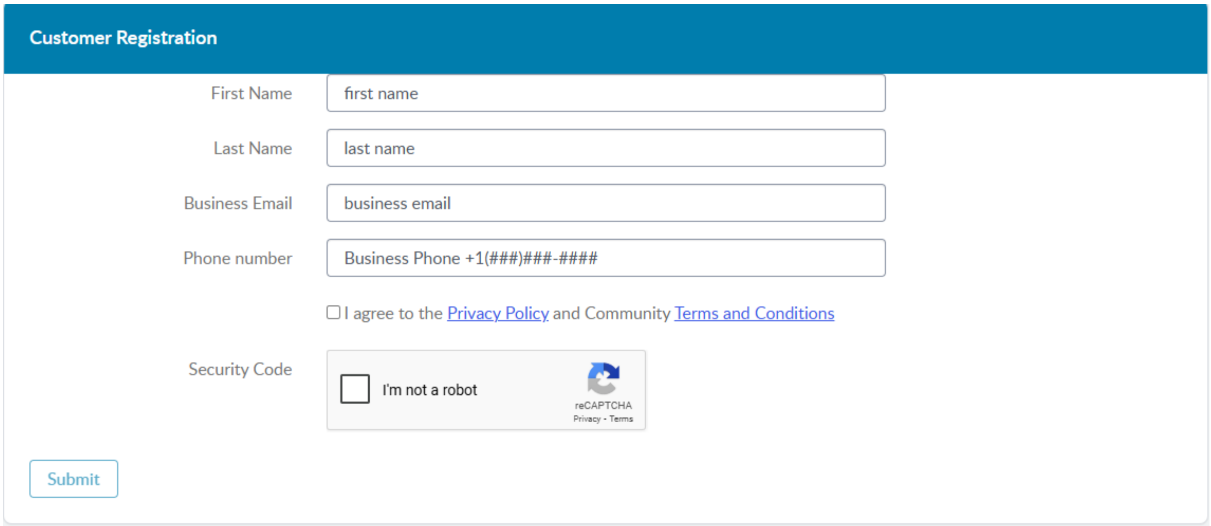
*****Please note this is a living document that will be updated with the progression of the contract. If there is something you feel is not accurate or should be added, please email vasmartnetea@ironbow.com*****

Appendix A | How to create a user ID for the Iron Bow portal

1.) For first time login please go [Here https://ironbow.servicenowservices.com/va](https://ironbow.servicenowservices.com/va)and select New User Registration.



2.) From there it will direct you to a page to fill out the needed information. Please note you must use your official VA email address to gain access to the tool. Any access requests that do not use their VA email will be automatically rejected from the system.



Customer Registration

First Name: first name

Last Name: last name

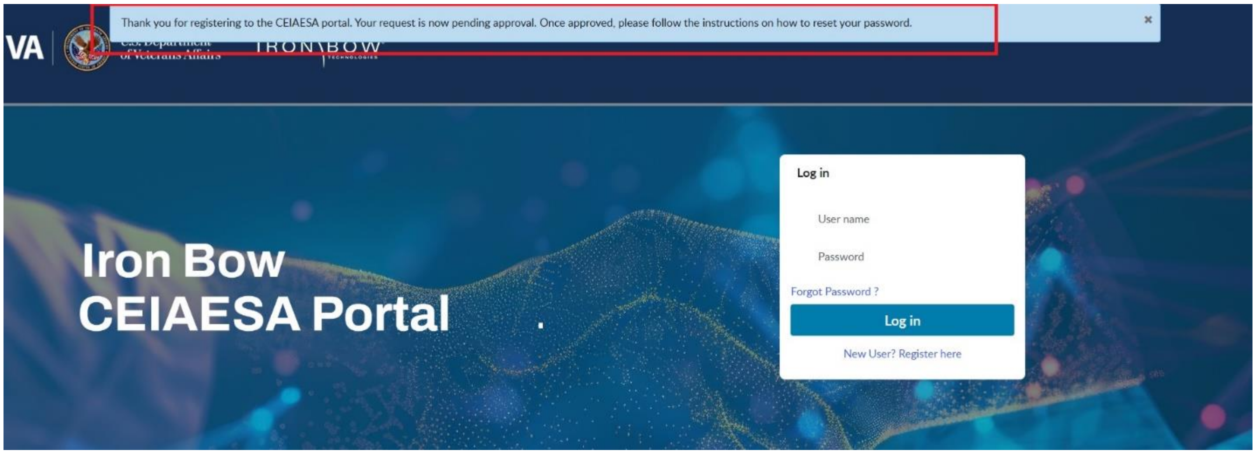
Business Email: business email

Phone number: Business Phone +1(###)###-####

□ I agree to the Privacy Policy and Community Terms and Conditions

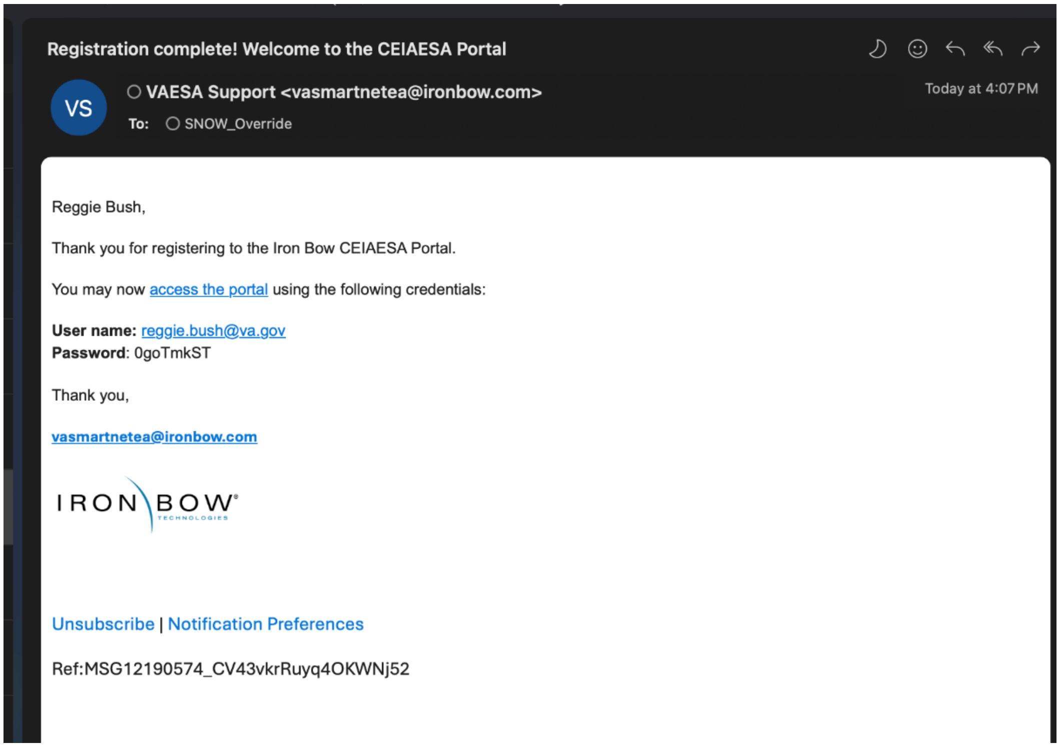
Security Code: □ I'm not a robot

3.) Once submitted the system will automatically push you to the login screen with a confirmation message as seen below. Your access request must be approved by a VA Super user before you can continue.



Thank you for registering to the CEIAESA portal. Your request is now pending approval. Once approved, please follow the instructions on how to reset your password.

4.) The system will send an automated email to the super users and portal administrators to approve or deny the request. If approved, you will receive an email with your username and temporary password. Example below. (If your request is denied you will receive a different message. If this is the case, please follow up with your leader for direction)



Registration complete! Welcome to the CEIAESA Portal

VS ○ VAESA Support <vasmartnetea@ironbow.com>

To: ○ SNOW_Override

Today at 4:07 PM

Reggie Bush,

Thank you for registering to the Iron Bow CEIAESA Portal.

You may now access the portal using the following credentials:

User name: reggie.bush@va.gov
Password: 0goTmkST

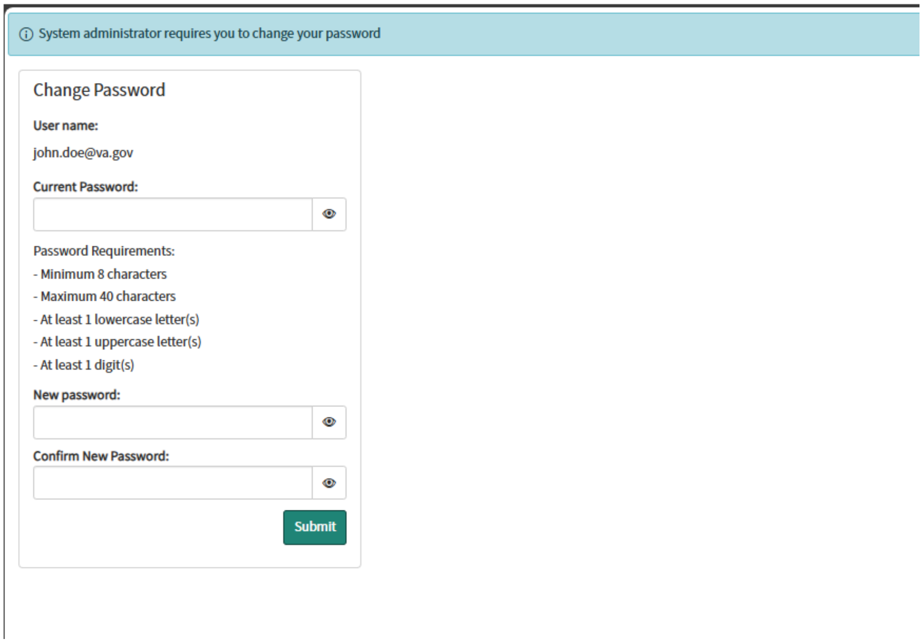
Thank you,

vasmartnetea@ironbow.com

Unsubscribe | Notification Preferences

Ref:MSG12190574_CV43vkrRuyq4OKWNj52

5.) Once Approved on your first login to the system you will be prompted to update/change your password to ensure that the system stays secure



ⓘ System administrator requires you to change your password

Change Password

User name:

john.doe@va.gov

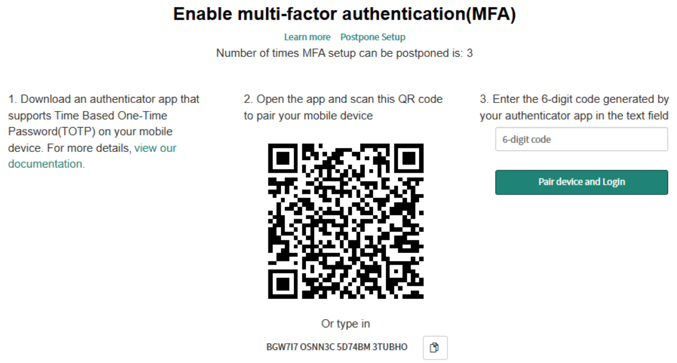
Current Password:

Password Requirements:
- Minimum 8 characters
- Maximum 40 characters
- At least 1 lowercase letter(s)
- At least 1 uppercase letter(s)
- At least 1 digit(s)

New password:

Confirm New Password:

6.) After changing your password, you will be prompted to register with an MFA tool for two factor authentication. The INITIAL authentication will require registration via a mobile app of your choice. (The VA preferred MFA tool is Microsoft Authenticator. You can also use any other authenticator such as Google Authenticator or Cisco Duo). Please note for initial authentication, the profile MUST be associated with your official VA Email address to register properly. After that, you will be able to obtain the authentication code via your mobile app or your registered VA email for authentication.



Enable multi-factor authentication(MFA)

Learn more Postpone Setup

Number of times MFA setup can be postponed is: 3

1. Download an authenticator app that supports Time Based One-Time Password(TOTP) on your mobile device. For more details, view our documentation.

2. Open the app and scan this QR code to pair your mobile device

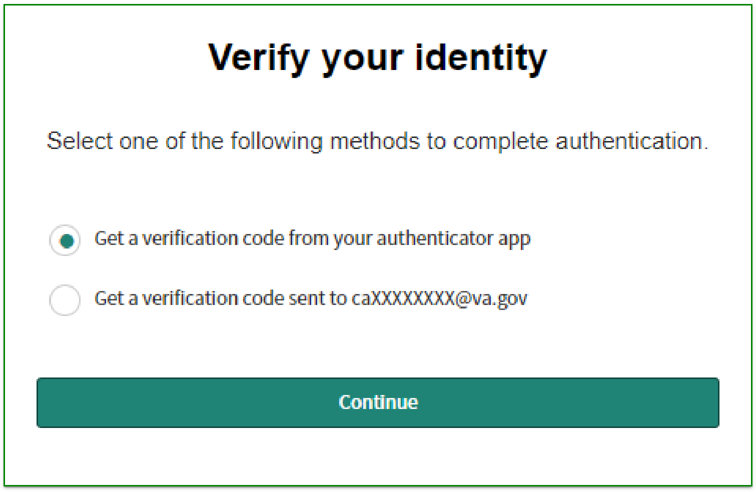
Or type in

BGW7I7 OSNN3C 5D74BM 3TUBHO

3. Enter the 6-digit code generated by your authenticator app in the text field

6-digit code

Pair device and Login



Verify your identity

Select one of the following methods to complete authentication.

● Get a verification code from your authenticator app

○ Get a verification code sent to caXXXXXXXX@va.gov

Continue

*****Once above steps have been complete your registration for the portal has been completed. For any escalations or problems please reach out to vasmartnetea@ironbow.com*****

Appendix B | Portal request/submissions and request types defined

Contract Move, Add, Change, Delete (MACD)

1.) Contract Move – This should be used for existing devices that are within the VA environment on a different contract/expired contract. For this type, please provide the old Contract Number the device serial number.
2.) Add – This should be used for Net New devices to the VA environment. For this request type please provide the device serial number instance number and the address where the new device will be installed. If this device is replacing a device currently active in the VA network, please provide the serial number of the device being replaced in the notes section of the case.
3.) Change – this action will be used for updating current devices on the CEIAESA Contract. These actions can be defined as address changes/updates/service level.
4.) Delete – This action type should be used for a device that's being decommissioned/replaced. Please note if this asset is being replaced, please ensure the new serial number is provided and note if the address will be different then what is listed on the legacy device.

All Change types will be subject to portal super user approval and case will be updated with notes for information requests and notification will be sent once approved.

Once approved by portal admin please allow up to 7 days for changes to be reflected in the portal.

Appendix C | Abbreviations and Definitions

CCO ID	Cisco Connection Online Identification. The user credentials created at Cisco.com to access device details from the Cisco Software Central website.
LDOS	Last Day of Support. Cisco's term that defines a date when a device will no longer be supported, replace, or create software updates for.
MCE	My Cisco Entitlements. A section of the Cisco Software Central website that provides the user access to details like what devices are assigned to their unit, cost of devices owned, and what date the device will enter LDOS status.
SDWAN	Software Defined Wide Area Network