Enhanced ACAM Cybersecurity and Supply Chain Risk Management Plan

Certification Filing System User Guide

Last Modified: November 8, 2023

Contents

About the Enhanced Alternative Connect America Cost Model (Enhanced ACAM) Cybersecurity and Supply Chain Risk Management Plan Certification Filing System

Carriers participating in the Enhanced Alternative Connect America Cost Model (Enhanced ACAM) program must submit cybersecurity and supply chain risk management plans to USAC through the E-file/Okta One Portal.

The FCC requires Enhanced ACAM carriers to implement operational cybersecurity and supply chain risk management plans by Jan. 1, 2024, which is the start of the support term for the new fund, and to file and certify these plans with USAC by Jan. 2, 2024, or within 30 days of receiving PRA approval, whichever is later. USAC will withhold 25 percent of monthly support from any carrier that fails to submit and certify its plans by the deadline until the carrier comes into compliance with the mandate.

The program requires all participating carriers to implement and submit to USAC:

- A cybersecurity plan that reflects the latest version of the Framework for Improving Critical Infrastructure Cybersecurity published by the National Institute of Standards and Technology (NIST), part of the U.S. Department of Commerce, and an established set of cybersecurity best practices, such as the standards and controls set out in the in the Cybersecurity & Infrastructure Security Agency (CISA) Cybersecurity Cross-sector Performance Goals and Objectives or the Center for Internet Security Critical Security Controls
- A supply chain risk management plan that incorporates key practices discussed in NISTIR 8276, Key Practices in Cyber Supply Chain Risk Management: Observations from Industry and related supply chain risk management guidance from NIST 800-161

Enhanced ACAM carriers must submit updated plans to USAC within 30 days if they make substantive modifications, such as a change in scope, risk mitigation strategies or organizational structure, and must certify in their annual Form 481 filings that they have maintained their plans and submitted any modifications.

Get Started

Prepare to Access the System

- Use Chrome (recommended), Firefox, or Edge when completing the Enhanced ACAM CSCRMP certification.
    - Users may encounter compatibility issues if using newer versions of Internet Explorer.
- Do not use browser's back and forward buttons when navigating between screens. Use One Portal system navigation buttons.
- Users should first clear the browser's cache if experiencing any issues with the application during login.

User Roles and Access to the Enhanced ACAM CSCRMP Certification System

Users with Service Provider Agent (SPA), Service Provider User (SPU), or Service Provider Officer (SPO) entitlements can access the Enhanced ACAM CSCRMP Certification System.
SPA and SPU users can only upload Cybersecurity or Supply Chain Risk Management Plans. SPA and SPU access is limited to one screen to upload and view the submitted plans.

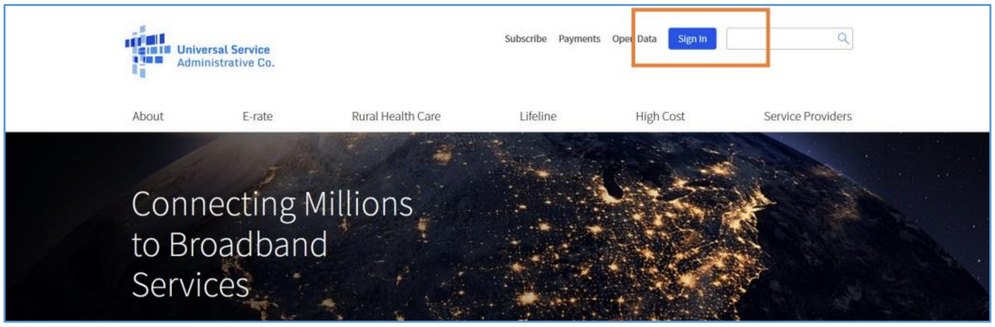
SPO users have access to all three screens where they can upload and view submitted plans, certify uploaded plans, and view the confirmation screen for the certified plans. Users will see the functionalities on screen based on their user roles.

Users should request entitlements from the carrier's 498 Officer. Form 498 Officers and/or 498 General Contacts should contact USAC about missing entitlements.

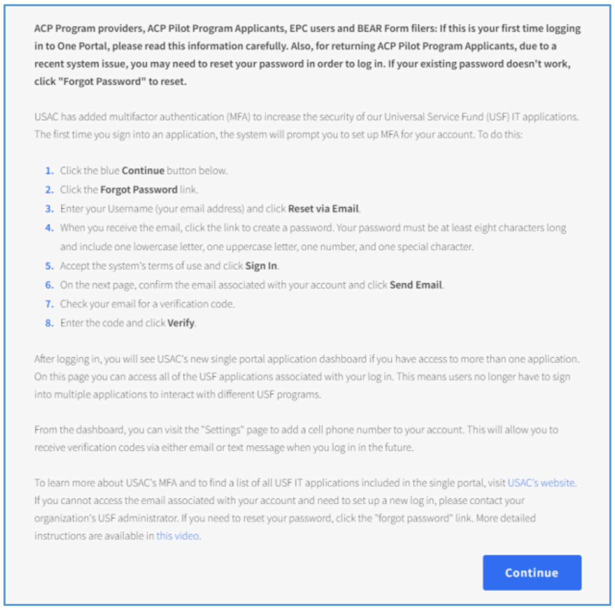
Access Details for the Enhanced ACAM CSCRMP Certification System

Once granted access, users can log in to the Enhanced ACAM CSCRMP Certification System and upload and/or certify the Cybersecurity or Supply Chain Risk Management plans. Follow the steps below to access the system.

- Visit USAC's website at usac.org and click the blue **Sign In** button in the upper right-hand corner of the homepage.



- First-time One Portal users will see a pop-up addressing EPC and BEAR Form filers. Click **Continue** to acknowledge.



ACP Program providers, ACP Pilot Program Applicants, EPC users and BEAR Form filers: If this is your first time logging in to One Portal, please read this information carefully. Also, for returning ACP Pilot Program Applicants, due to a recent system issue, you may need to reset your password in order to log in. If your existing password doesn't work, click "Forgot Password" to reset.

USAC has added multifactor authentication (MFA) to increase the security of our Universal Service Fund (USF) IT applications. The first time you sign into an application, the system will prompt you to set up MFA for your account. To do this:

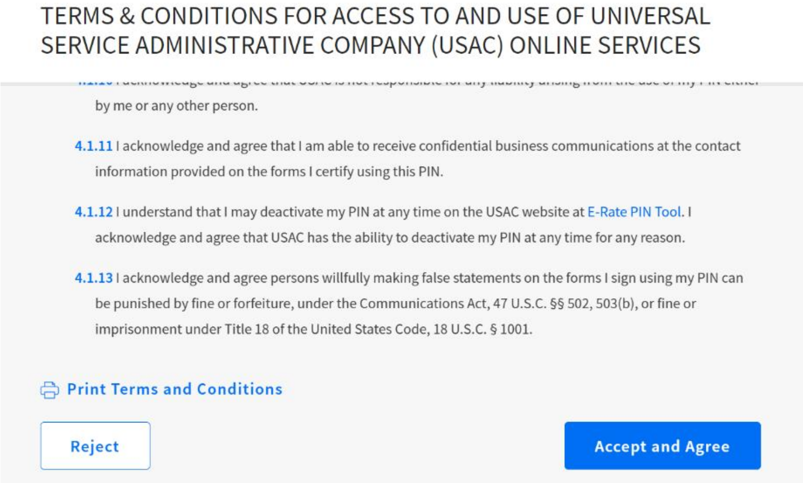
1. Click the blue **Continue** button below.
2. Click the **Forgot Password** link.
3. Enter your Username (your email address) and click **Reset via Email**.
4. When you receive the email, click the link to create a password. Your password must be at least eight characters long and include one lowercase letter, one uppercase letter, one number, and one special character.
5. Accept the system's terms of use and click **Sign In**.
6. On the next page, confirm the email associated with your account and click **Send Email**.
7. Check your email for a verification code.
8. Enter the code and click **Verify**.

After logging in, you will see USAC's new single portal application dashboard if you have access to more than one application. On this page you can access all of the USF applications associated with your log in. This means users no longer have to sign into multiple applications to interact with different USF programs.

From the dashboard, you can visit the "Settings" page to add a cell phone number to your account. This will allow you to receive verification codes via either email or text message when you log in in the future.

To learn more about USAC's MFA and to find a list of all USF IT applications included in the single portal, visit USAC's website. If you cannot access the email associated with your account and need to set up a new log in, please contact your organization's USF administrator. If you need to reset your password, click the "forgot password" link. More detailed instructions are available in this video.

- The next screen outlines the terms and conditions for accessing and using USAC Online Services. Click **Accept and Agree** to advance to USAC's One Portal System. Users may print the Terms and Conditions or reject them.



TERMS & CONDITIONS FOR ACCESS TO AND USE OF UNIVERSAL SERVICE ADMINISTRATIVE COMPANY (USAC) ONLINE SERVICES

4.1.10 I acknowledge and agree that USAC is not responsible for any liability arising from the use of my PIN either by me or any other person.

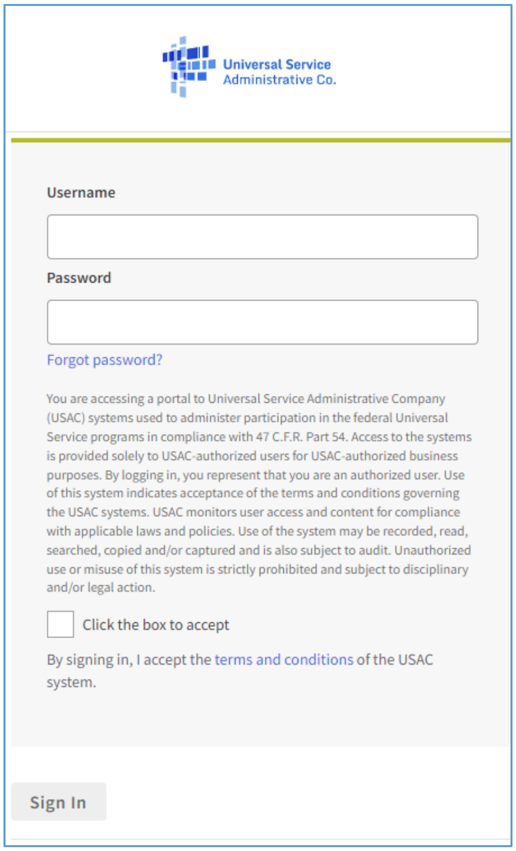
4.1.11 I acknowledge and agree that I am able to receive confidential business communications at the contact information provided on the forms I certify using this PIN.

4.1.12 I understand that I may deactivate my PIN at any time on the USAC website at E-Rate PIN Tool. I acknowledge and agree that USAC has the ability to deactivate my PIN at any time for any reason.

4.1.13 I acknowledge and agree persons willfully making false statements on the forms I sign using my PIN can be punished by fine or forfeiture, under the Communications Act, 47 U.S.C. §§ 502, 503(b), or fine or imprisonment under Title 18 of the United States Code, 18 U.S.C. § 1001.

- Enter the username and password. Select the checkbox to accept the disclaimer. The **Sign In** button will only become available once this box is checked.

- Click **Sign In** to access One Portal.

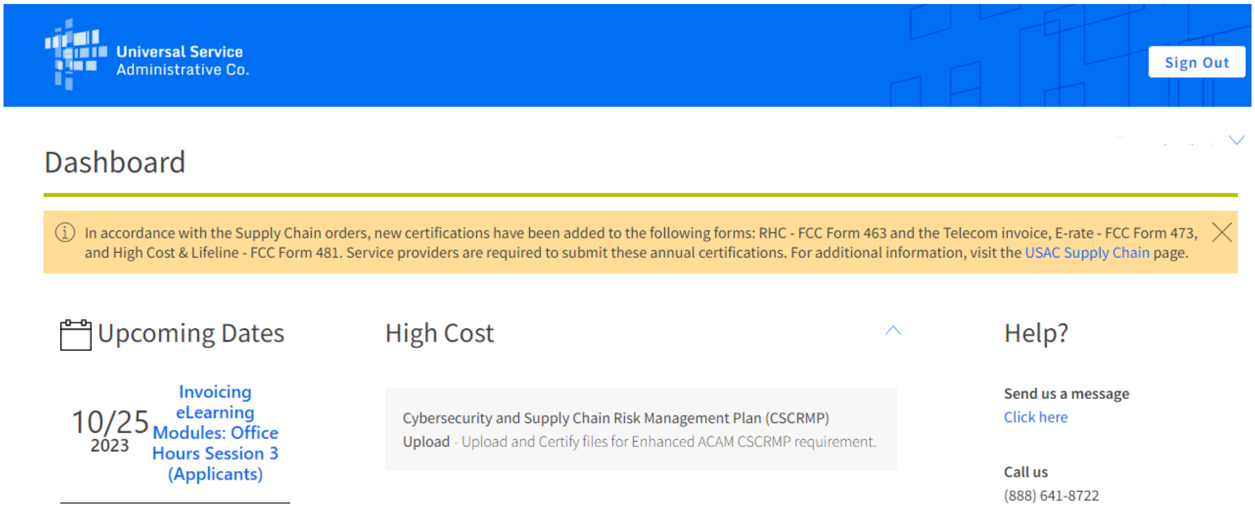


You are accessing a portal to Universal Service Administrative Company (USAC) systems used to administer participation in the federal Universal Service programs in compliance with 47 C.F.R. Part 54. Access to the systems is provided solely to USAC-authorized users for USAC-authorized business purposes. By logging in, you represent that you are an authorized user. Use of this system indicates acceptance of the terms and conditions governing the USAC systems. USAC monitors user access and content for compliance with applicable laws and policies. Use of the system may be recorded, read, searched, copied and/or captured and is also subject to audit. Unauthorized use or misuse of this system is strictly prohibited and subject to disciplinary and/or legal action.

□ Click the box to accept

By signing in, I accept the terms and conditions of the USAC system.

- Click on **Cybersecurity and Supply Chain Risk Management Plan (CSCRMP) Upload** under the High Cost header. Users may need to click the arrow next to **High Cost** to expand the section to see the CSCRMP system listed.



Dashboard

ⓘ In accordance with the Supply Chain orders, new certifications have been added to the following forms: RHC - FCC Form 463 and the Telecom invoice, E-rate - FCC Form 473, and High Cost & Lifeline - FCC Form 481. Service providers are required to submit these annual certifications. For additional information, visit the USAC Supply Chain page.

Upcoming Dates

10/25 2023 Invoicing eLearning Modules: Office Hours Session 3 (Applicants)

High Cost

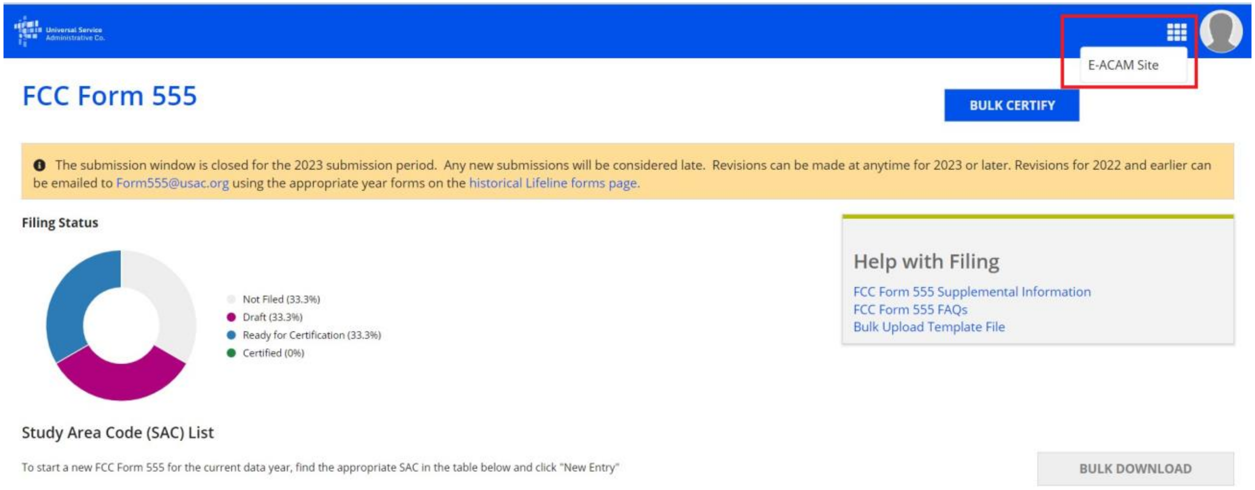
Cybersecurity and Supply Chain Risk Management Plan (CSCRMP) Upload - Upload and Certify files for Enhanced ACAM CSCRMP requirement.

Help?

Send us a message
Click here

Call us
(888) 641-8722

- Form 555 users only: After clicking **Cybersecurity and Supply Chain Risk Management Plan (CSCRMP) Upload**, users may land on the FCC Form 555 page. From there, users should click the navigation icon ▦ and select **Enhanced ACAM Site** to enter the Enhanced ACAM CSCRMP Certification System.



FCC Form 555

❶ The submission window is closed for the 2023 submission period. Any new submissions will be considered late. Revisions can be made at anytime for 2023 or later. Revisions for 2022 and earlier can be emailed to Form555@usac.org using the appropriate year forms on the historical Lifeline forms page.

Filing Status

- ○ Not Filed (33.3%)
- ● Draft (33.3%)
- ● Ready for Certification (33.3%)
- ● Certified (0%)

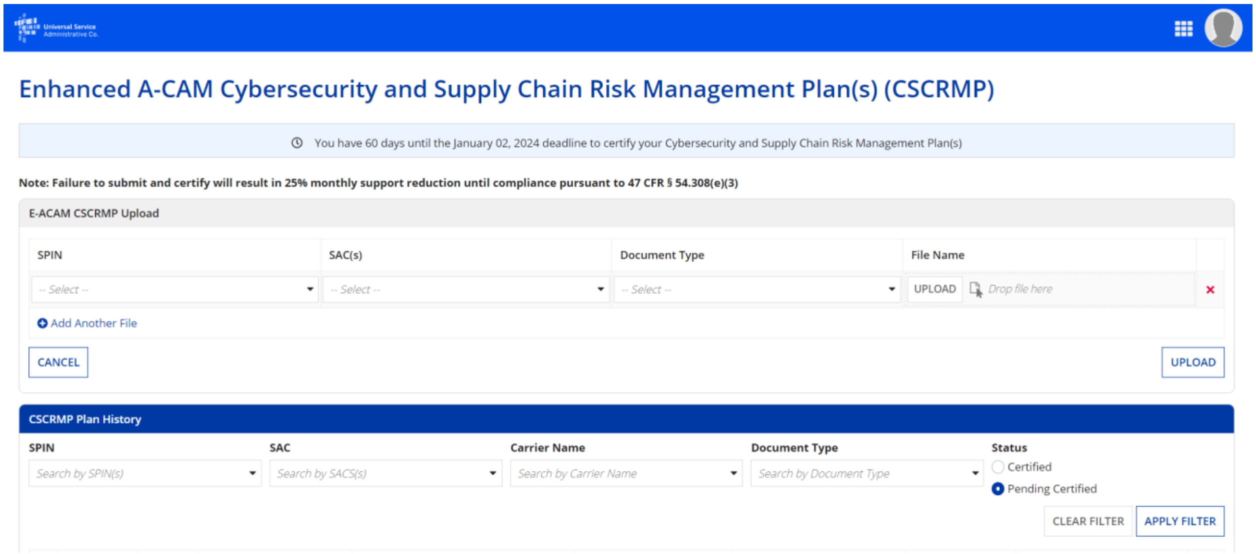
Help with Filing

FCC Form 555 Supplemental Information
FCC Form 555 FAQs
Bulk Upload Template File

Study Area Code (SAC) List

To start a new FCC Form 555 for the current data year, find the appropriate SAC in the table below and click "New Entry"

- The **Enhanced ACAM Cybersecurity and Supply Chain Risk Management Plan(s) (CSCRMP)** screen will be visible upon successful log-in.



Enhanced A-CAM Cybersecurity and Supply Chain Risk Management Plan(s) (CSCRMP)

You have 60 days until the January 02, 2024 deadline to certify your Cybersecurity and Supply Chain Risk Management Plan(s)

Note: Failure to submit and certify will result in 25% monthly support reduction until compliance pursuant to 47 CFR § 54.308(e)(3)

E-ACAM CSCRMP Upload

SPIN	SAC(s)	Document Type	File Name
-- Select --	-- Select --	-- Select --	UPLOAD Drop file here

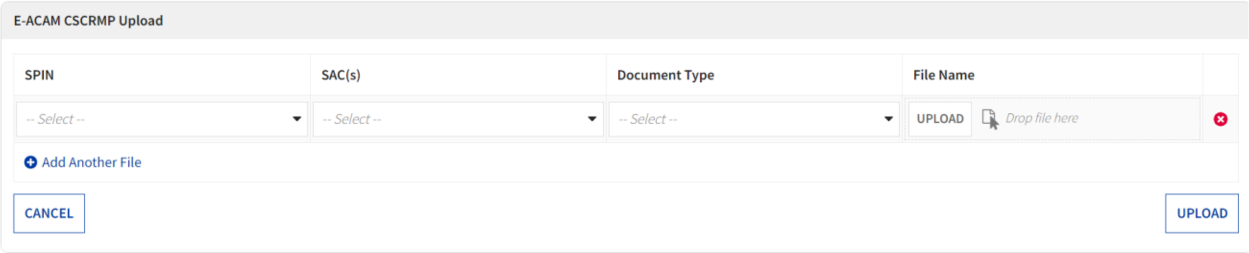
CSCRMP Plan History

SPIN	SAC	Carrier Name	Document Type	Status
Search by SPIN(s)	Search by SACS(s)	Search by Carrier Name	Search by Document Type	○ Certified ● Pending Certified

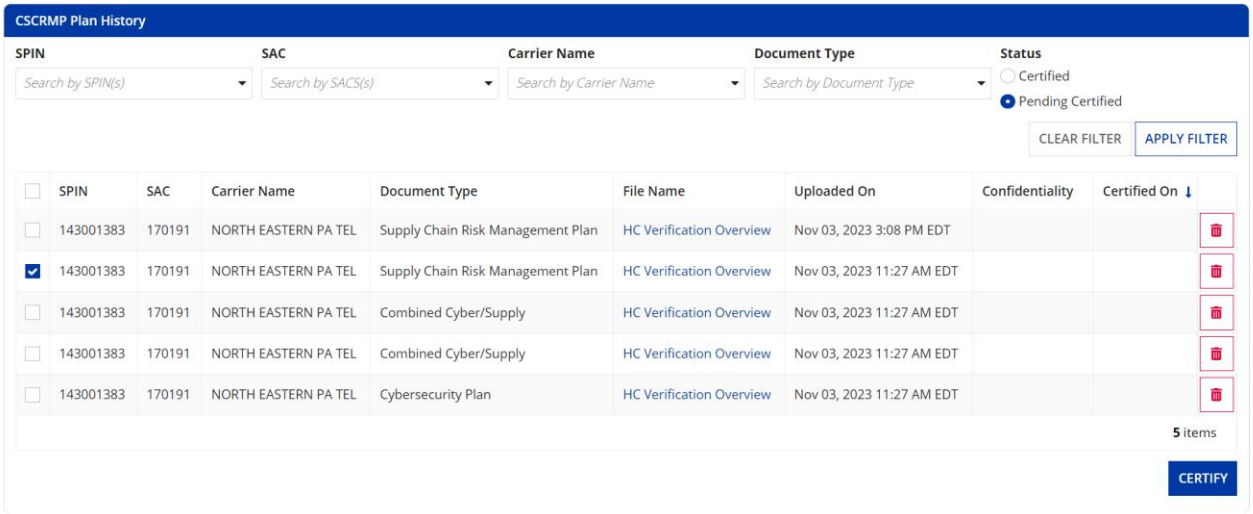
1. Enhanced ACAM File Upload and History Screen Overview

There are two sections on this screen.

- The first section is called **Enhanced ACAM CSCRMP Upload** and is used to upload files. This section has a total of four required fields:
    - The **SPIN** dropdown field contains a list of 498 IDs to which the user has entitlements
    - The **SAC(s)** dropdown field contains a list of SAC(s) that corresponds to the SPIN displayed in the SPIN field
    - The **Document Type** field shows the plan type that users can select to upload. The three options are:
        - Cybersecurity Plan
        - Supply Chain Risk Management Plan
        - Combined Cyber/Supply
    - The **File Name** field allows the user to select and upload plan files
        - The system only allows the following file types: PDF, xlsx, and xls
        - File sizes cannot exceed 20 MB



- The second section is called **CSCRMP Plan History** and displays the upload and certification history. This section has a table with the following fields: **SPIN, SAC, Carrier Name, Document Type, File Name, Uploaded On, Confidentiality**, and **Certified On.** Users can filter and sort the records shown based on certain criteria. The following columns permit filters: **SPIN, SAC**, **Carrier Name, Document Type**, and **Status**.



CSCRMP Plan History

SPIN: Search by SPIN(s)

SAC: Search by SACS(s)

Carrier Name: Search by Carrier Name

Document Type: Search by Document Type

Status: ○ Certified ● Pending Certified

	SPIN	SAC	Carrier Name	Document Type	File Name	Uploaded On	Confidentiality	Certified On ↓	
□	143001383	170191	NORTH EASTERN PA TEL	Supply Chain Risk Management Plan	HC Verification Overview	Nov 03, 2023 3:08 PM EDT			🗑
☑	143001383	170191	NORTH EASTERN PA TEL	Supply Chain Risk Management Plan	HC Verification Overview	Nov 03, 2023 11:27 AM EDT			🗑
□	143001383	170191	NORTH EASTERN PA TEL	Combined Cyber/Supply	HC Verification Overview	Nov 03, 2023 11:27 AM EDT			🗑
□	143001383	170191	NORTH EASTERN PA TEL	Combined Cyber/Supply	HC Verification Overview	Nov 03, 2023 11:27 AM EDT			🗑
□	143001383	170191	NORTH EASTERN PA TEL	Cybersecurity Plan	HC Verification Overview	Nov 03, 2023 11:27 AM EDT			🗑

5 items

Files uploaded in the Enhanced ACAM CSCRMP Upload section will appear in the **CSCRMP Plan History** section table with the Confidentiality and Certified On columns blank. Users can download the file(s) by clicking the hyperlink in the File Name column. Users can delete submitted plans by clicking the trash can icon in the last column. **SPO** users will see checkboxes in the first column in the CSCRMP Plan History table The **CERTIFY** button will appear at the bottom once an **SPO** user selects the file(s) to certify by clicking the corresponding check box.

File Naming Convention for CSCRMP Upload:

When uploading a cybersecurity or supply chain risk management plan, carriers should use a description of document as the file name. For example, if Carrier X submits a cybersecurity plan, the file should be named "Carrier X Cybersecurity Plan." Should an existing plan need to be modified, carriers should use the same file name as the original submitted plan and add a version number. For example, if the original file name is "Carrier X Cybersecurity Plan" then the modified file should be named "Carrier X Cybersecurity Plan V2".

2. Enhanced ACAM Certification Screen Overview

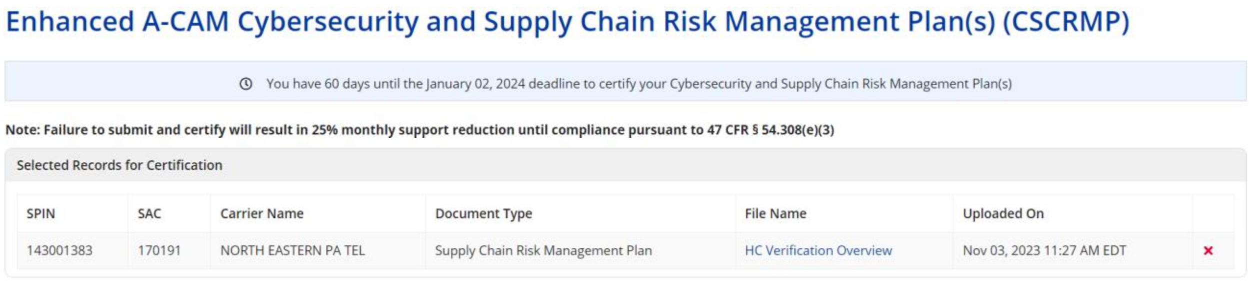
The Certification screen is only available to **SPO** users and has two sections.

- The first section is called **Selected Records for Certification** and displays all the records selected to certify in the previous screen.

  The section lists a table with six fields:

  - The **SPIN** column shows the list of SPIN value(s) selected from the previous screen
  - The **SAC** column shows the list of SAC value(s) selected from the previous screen

- ○ The **Carrier Name** column shows the Eligible Telecommunication Carriers (ETCs) corresponding to the SACs selected from the previous screen
- ○ The **Document Type** column shows the plan(s) type the user selected to upload from the previous screen.
- ○ The **File Name** column shows the name of the uploaded file(s)
- ○ The **Uploaded On** column shows the date the plan(s) were uploaded to the CSCRMP Plan History table in the previous screen



Enhanced A-CAM Cybersecurity and Supply Chain Risk Management Plan(s) (CSCRMP)

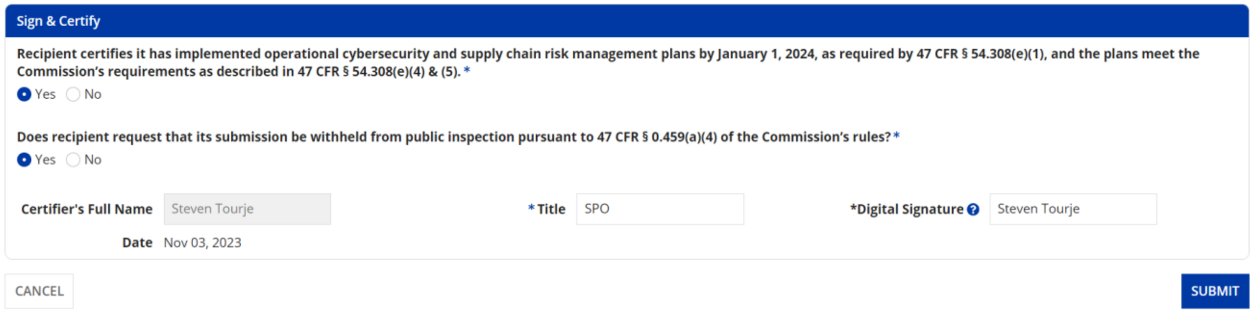
You have 60 days until the January 02, 2024 deadline to certify your Cybersecurity and Supply Chain Risk Management Plan(s)

Note: Failure to submit and certify will result in 25% monthly support reduction until compliance pursuant to 47 CFR § 54.308(e)(3)

Selected Records for Certification

SPIN	SAC	Carrier Name	Document Type	File Name	Uploaded On	
143001383	170191	NORTH EASTERN PA TEL	Supply Chain Risk Management Plan	HC Verification Overview	Nov 03, 2023 11:27 AM EDT	×

- The second section is called **Sign & Certify.** This section contains two responses that are required to submit the certification. The Certifier's Full Name and the Digital Signature must match to activate the **SUBMIT** button. Title is a required field.



Sign & Certify

Recipient certifies it has implemented operational cybersecurity and supply chain risk management plans by January 1, 2024, as required by 47 CFR § 54.308(e)(1), and the plans meet the Commission's requirements as described in 47 CFR § 54.308(e)(4) & (5). *

● Yes ○ No

Does recipient request that its submission be withheld from public inspection pursuant to 47 CFR § 0.459(a)(4) of the Commission's rules? *

● Yes ○ No

Certifier's Full Name Steven Tourje

*** Title** SPO

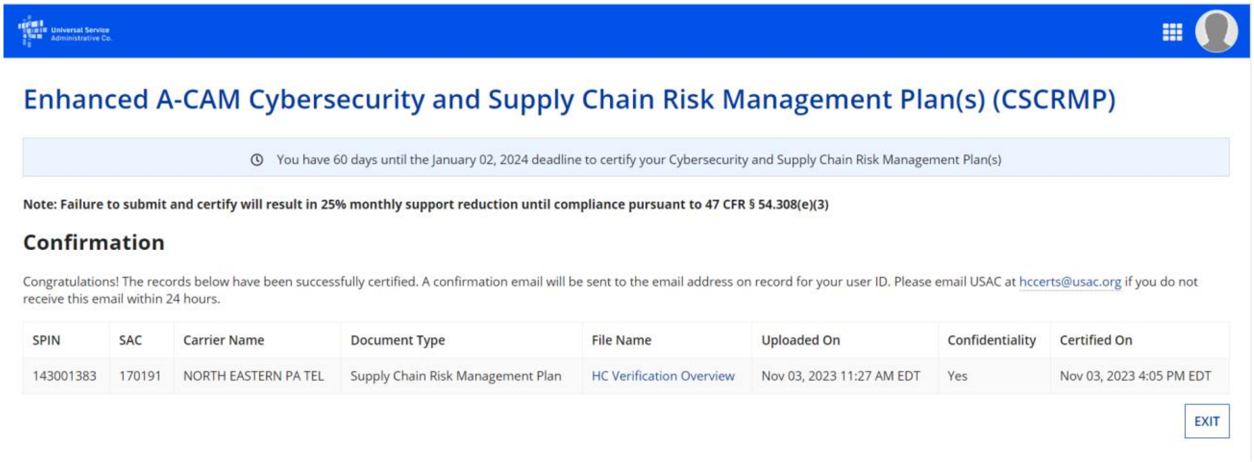
***Digital Signature** Steven Tourje

Date Nov 03, 2023

3. Enhanced ACAM Certification Confirmation Screen Overview

The Certification Confirmation screen is only available to **SPO** users and has one section containing the table of certified records. The table has eight fields:

- The **SPIN** column shows the list of SPIN value(s) selected from the previous screen
- The **SAC** column shows the list of SAC value(s) selected from the previous screen
- The **Carrier Name** column shows the ETCs corresponding to the SACs selected from the previous screen
- The **Document Type** column shows the plan(s) type selected for upload from the previous screen
- The **File Name** column shows the name of the uploaded file(s)
- The **Uploaded On** column shows the date the plan(s) were uploaded to the CSCRMP Plan History table in the previous screen
- The **Confidentiality** column shows the answer selected for the Confidentiality question on the Certification screen
- The **Certified On** column shows the date the file(s) were certified



Enhanced A-CAM Cybersecurity and Supply Chain Risk Management Plan(s) (CSCRMP)

You have 60 days until the January 02, 2024 deadline to certify your Cybersecurity and Supply Chain Risk Management Plan(s)

Note: Failure to submit and certify will result in 25% monthly support reduction until compliance pursuant to 47 CFR § 54.308(e)(3)

Confirmation

Congratulations! The records below have been successfully certified. A confirmation email will be sent to the email address on record for your user ID. Please email USAC at hccerts@usac.org if you do not receive this email within 24 hours.

SPIN	SAC	Carrier Name	Document Type	File Name	Uploaded On	Confidentiality	Certified On
143001383	170191	NORTH EASTERN PA TEL	Supply Chain Risk Management Plan	HC Verification Overview	Nov 03, 2023 11:27 AM EDT	Yes	Nov 03, 2023 4:05 PM EDT

4. Enhanced ACAM Certification Confirmation Email

SPO users will receive a copy of the Certification Confirmation at the e-mail address associated with the User ID.

Need Help? Contact Us!

Contact the High Cost Customer Service Center at (844) 357-0408 Monday–Friday 8 a.m. to 8 p.m. ET or email HCQuestions@usac.org.