



Customs Trade Partnership Against Terrorism

CTPAT Portal

User Manual

April 11, 2025

Revision 1.0

Table of Contents

Terms and Definitions ..... 1 - 5

Introduction 5

- Joining CTPAT and Basic Navigation 5-6
- Creating a CTPAT Account ..... 6 - 9
- Eligibility Requirements 9
- Business Information ..... 9 - 14
- International Arrangements ..... 11 - 13
- Security Profile ..... 14 - 23
- Partner Document Exchange (Uploading Documents) 24
- Status Verification Interface (SVI, Partner Monitoring) ..... 25 - 31
- Validation and 90-day response ..... 31 – 33
- Public Document Library ..... 33 – 34
- Trouble Shooting 35

Terms and Definitions

AEO	Authorized Economic Operator. A party involved in the international movement of goods in whatever function that has been approved by a customs administration that complies with World Customs Organization (WCO) or equivalent supply chain security standards. AEO programs are intended to enhance security and facilitate legitimate trade.
AQUA Lane	Advanced Qualified Unlading Approval. A benefit available for low-risk sea carriers in the CTPAT program. It allows vessels under the control of the CTPAT carrier to request permission to unlade cargo on arrival and prior to being cleared by U.S. Customs and Border Protection (CBP).
CBSA	Canada Border Services Agency. The Canadian government agency which administers the Authorized Economic Operator program Partners in Protection ("PIP").
Certified	Status bestowed once an applicant has met eligibility requirements, passed initial vetting and provided answers to a Security Profile confirming adherence to the CTPAT Minimum-Security Criteria (MSC). Also known as Tier I status.
Certified, Exceeding	Status for CTPAT importers and select exporters who meet and exceed the Minimum-Security Criteria (MSC), as well as lead industry with several "Best Practices." This status is granted by CTPAT Headquarters only on a case-by-case basis, after the partner successfully completes a CTPAT validation with verified "Best Practices" and no Actions Required. Also known as Tier III status.
Certified, Validated	Status of CTPAT partners who have met the Minimum-Security Criteria (MSC) and successfully completed a validation. Also known as Tier II status.
COAC	Commercial Customs Operations Advisory Committee on Commercial Operations of Customs and Border Protection (COAC). COAC is a 20-member advisory council composed of members of the Trade. The council advises the Department of Homeland Security on the commercial operations of CBP and related DHS functions. COAC has Subcommittees and Leads on: Secure Trade Lanes, Intelligent Enforcement, Next Generation Facilitation, and Rapid Response.
Company Officer	A high-level company officer who holds an office of authority and acts in an official capacity on behalf of a company. A Company Officer would have the authority to submit the CTPAT Security Profile within the CTPAT Portal account.
Company Profile	The portion of a CTPAT Portal Application or CTPAT Account that contains basic company information, such as addresses, points of contact, and brief description of company operations.
Consultant	A third party who provides professional or expert advice for a client, the company. However, the consultant is unable to act in an official capacity making decisions for the client. A consultant

	may submit information to CTPAT for a client, as long as the client is aware of what is being submitted and accurately reflects the client's security procedures.
CTPAT	Customs Trade Partnership Against Terrorism. A voluntary partnership between the U.S. Government and members of the trade based on the security of international supply chains with a focus on anti-terrorism. The program is led by U.S. Customs and Border Protection (CBP).
CTPAT Application	A CTPAT application is the creation and submission of a CTPAT account and subsequent required information in the CTPAT Portal.
CTPAT Partner	A company that has achieved Certified status with the CTPAT program, continues to meet the eligibility and vetting requirements, and adheres to the Partner Agreement.
Customs and Border Protection (CBP)	One of the U.S. Department of Homeland Security's largest and most complex components, with a priority mission of keeping terrorists and their weapons out of the U.S. CBP also is responsible for securing and facilitating trade and travel while enforcing hundreds of U.S. regulations, including immigration and drug laws.
Eligibility Requirements	Requirements that must be met by CTPAT program applicants at the time of application for CTPAT membership.
FAST	The Free and Secure Trade program. A commercial clearance program for known low-risk shipments entering the United States from Canada and Mexico. This program allows expedited processing through dedicated vehicle lanes for commercial carriers who have fulfilled certain eligibility requirements. FAST vehicle lanes process cargo at land border ports of entry that serve commercial cargo. Participation in FAST requires that every link in the supply chain, from manufacturer to carrier to driver to importer, is CTPAT certified.
FMC	U.S. Federal Maritime Commission. An independent federal agency responsible for regulating the U.S. international ocean transportation system for the benefit of U.S. exporters, importers, and the U.S. consumer.
IATA	International Air Transport Association ("IATA"). A global trade association for the airline industry. IATA has 340 member airlines in 120 countries, representing over 80% of the world's total air traffic.
IOR – Importer of Record Number	The IOR is a unique identifier assigned by CBP to individuals or entities responsible for ensuring imported goods meet all legal and regulatory requirements.
Login.gov	Login.gov is a secure, government provided service that allows the public to access various government websites and applications using a single, shared account and password. It helps protect information with two-factor authentication.
Minimum Security Criteria	Security standards that companies must meet to be accepted as a partner in CTPAT.

MRA	Mutual Recognition Arrangement. A country's government formally recognizing the Authorized Economic Operator (AEO) program of another country's government and thereby granting benefits to the respective country's AEOs members.
PDF	Portable Document Format. How information is formatted when exporting information from a CTPAT Account. Such documents are saved electronically using the ".pdf" file extension. An example of this is a Security Profile that has been uploaded to the Partner Document Exchange after approval.
PGA's	Partner Government Agency (e.g., TSA, FDA)
PIP	Partners In Protection, an Authorized Economic Operator (AEO) program administered by the Canadian Border Services Agency (CBSA).
Point of Contact	The Point of Contact (POC) is any person listed as a contact or user within CTPAT's Portal. The POCs are the only people authorized to work with the CTPAT program on the company's behalf. Points of Contact must be empowered to make decisions and policy changes regarding the Partner's security procedures.
Portal (the CTPAT Portal)	The CTPAT Portal is designed to streamline applications to the CTPAT and Trade Compliance programs, add functionality requested by CTPAT Partners, and meet DHS mandated security requirements. The Portal provides flexibility to adapt to future data requirements and administer multiple partnership programs, e.g., CTPAT and CTPAT Trade Compliance within a single site.
Risk Assessment	Risk Assessment is a process of identifying, analyzing, and evaluating potential hazards and risks associated within the supply chain and potential impact of those risks along with developing strategies to mitigate those risks. For example, natural disasters, civil unrest, acts of terrorism, labor strikes may all be areas of risk that a business considers when moving cargo. For CTPAT purposes, a Risk Assessment is narrower in scope and may be defined as an International Supply Chain Security Risk Assessment that examines security threats and vulnerabilities associated with a CTPAT Partner's international supply chain in each node of the chain from the point of origin where the goods are manufactured, until they reach their final destination for distribution. The assessment should also include a plan to mitigate the risks identified in the assessment.
SCAC	Standard Carrier Alpha Code. A unique identification code used to identify transportation companies (highway carriers). Typically, four alphabetic letters long, the SCAC was developed by the National Motor Freight Traffic Association in the 1960s to help the transportation industry computerize data and records.
Security Profile Annual Review	The account review that must be conducted on an annual basis by the Partner within the 90 days prior to the Partner's "Anniversary Date" shown in the Portal. This process includes a review and update of the Security Profile (Business Details and entire CTPAT Account should also be updated), to ensure that the information contained therein remains current and

	accurate. The company officer must sign the Membership Agreement in the Portal, prior to submitting the Security Profile to complete the Annual Review. The SCSS reviews the Security Profile in order to verify that the partner still meets the CTPAT Minimum Security Criteria.
Security Profile	The Security Profile is the Applicant/Partner's written declaration of adherence to CTPAT's Minimum-Security Criteria (MSC), and procedures used throughout the international supply chain. The Security Profile is maintained in the CTPAT Portal account and must be reviewed by the CTPAT Partners on at least an annual basis as part of its required Annual Review of Security Profile. The information provided in the Security Profile is verified during the validation process.
Supply Chain Security Specialist (SCSS)	The CBP CTPAT representative who manages the accounts of CTPAT Partners and works with their assigned companies to achieve and maintain CTPAT certification.
SVI – Status Verification Interface	Online tool used by CTPAT Partners to verify membership and status of other Partners in the CTPAT program.
Trade Compliance	The CTPAT Trade Compliance Program includes importers who can demonstrate their readiness to assume the responsibility of managing and monitoring their own compliance through self-assessment. Importers accepted into the CTPAT Trade Compliance Program receive tangible benefits, and their participation allows CBP to redirect resources and focus on higher-risk and unknown importers. To be eligible, the importer must be a current Tier II (validated) or Tier III (exceeding) member of the CTPAT Program. Importers must apply and undergo an application evaluation conducted by the Office of Trade, Trade Regulatory Audit. If accepted into the program, the importer is assigned a National Account Manager (NAM), who acts as an advisor and liaison between CBP and the importer
Trade User	A non-government trade partner who has a user account in the Portal.
TUI	Trade User Interface. This is how the trade partner interacts with the CTPAT Portal.
Validation	A verification of company security measures and supply chain security practices based on the CTPAT minimum-security criteria. Validations are mandated by the SAFE Port Act to take place at least every four years but may be conducted more frequently based on risk.

Introduction

The CTPAT web Portal is continually evolving to meet the demands of the trade environment, technology and new trends in supply chain security. This manual details steps taken to submit an accurate and complete CTPAT application. It will also enable partners in the program the ability to take advantage of foreign AEO cargo facilitation benefits through the Mutual Recognition Arrangement section of the CTPAT Portal.

CTPAT is also working in partnership with other U.S. Government / trade partnership programs and other departments within CBP and DHS such as the Transportation Security Administration (TSA), to assist with air with carrier validations, and with the Agriculture Programs and Trade Liaison (APTL), to advise and lead efforts with the newly implemented agricultural requirements of the MSC. The Portal has advanced to allow for growing relationships with foreign government AEO programs which expands benefits to foreign ports of entry.

Portal Account Management

SYSTEMS REQUIREMENTS

- Google Chrome (preferred) or Microsoft Edge to access Portal
- JAVA updates
- Ensure all company profile information has been updated (*Difficulty using Portal applications will result if not up to date*)

Joining CTPAT

The application process for the CTPAT program is initiated online. A company representative must complete the application on a secure website called the CTPAT Portal. There are two main components to the application process: the Business Details and the Security Profile. The Business Details section of the application asks for company history, addresses, contact information, business identifiers, etc. Once the required application information is completed and the "Submit" button is clicked an account is then created in the CTPAT Portal. The submission must occur within 90 days of initiation of the application, or the account will be automatically withdrawn. Once the account has been created, the company representative will then be required to answer CTPAT's Minimum-Security Criteria (MSC) questions and confirm adherence to the requirements within the Security Profile. All application information is reviewed by a Supply Chain Security Specialist (SCSS) who will be assigned to the company account. The SCSS reviews the submitted application and determines the company's eligibility to join the CTPAT program.

After the application is reviewed and approved, the company will be certified (Tier I) in the CTPAT program and may start receiving cargo facilitation benefits. At this time, the SCSS assigned to the account will contact the main point of contact to initiate a site visit(s), as a part of the company's "validation. A validation is required because the SCSS must physically verify that the information submitted in the application is accurate and in practice. Once an onsite physical validation is completed, and the SCSS has found the company to be in compliance with CTPAT requirements, the company account status may be updated to validated (Tier II) and begin receiving additional benefits of the CTPAT program. Below, are the necessary steps to apply for the CTPAT program:

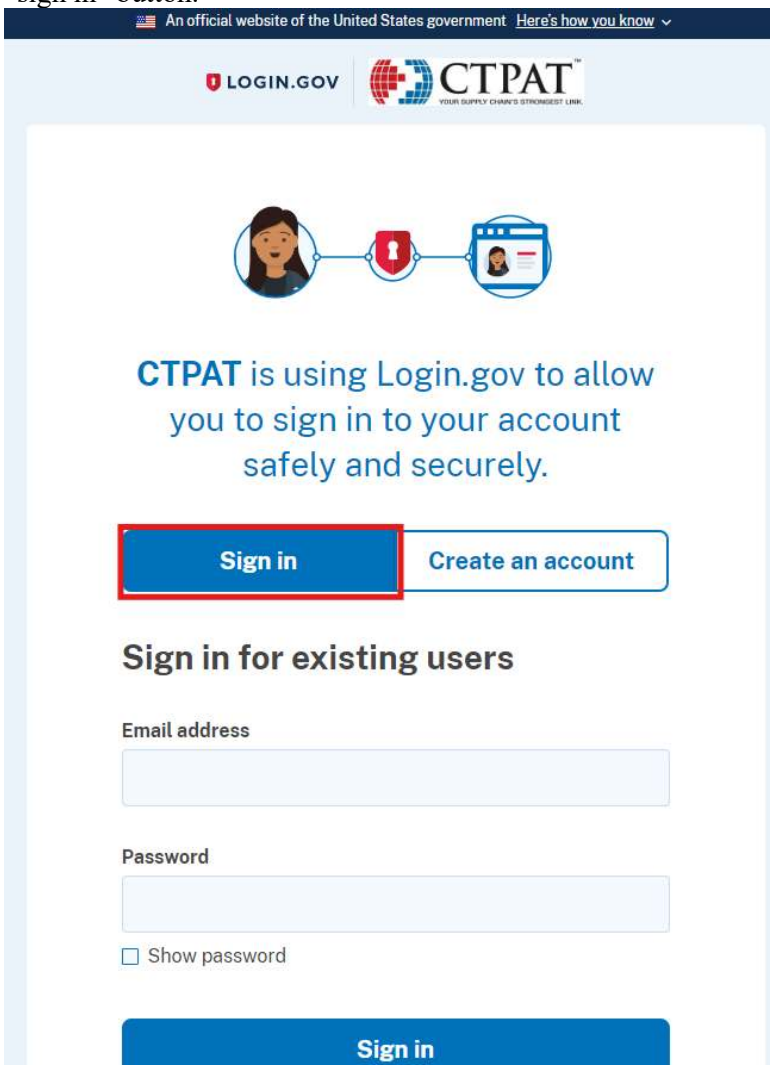
1. First, create a login.gov account. Instructions for creating an account can be found here. When creating this account, please ONLY use the email address you plan to use in the CTPAT Portal. **Do not** add any alternate or recovery email addresses, or it may disrupt your access to the CTPAT Portal.

2. Next, navigate to the CTPAT Portal.

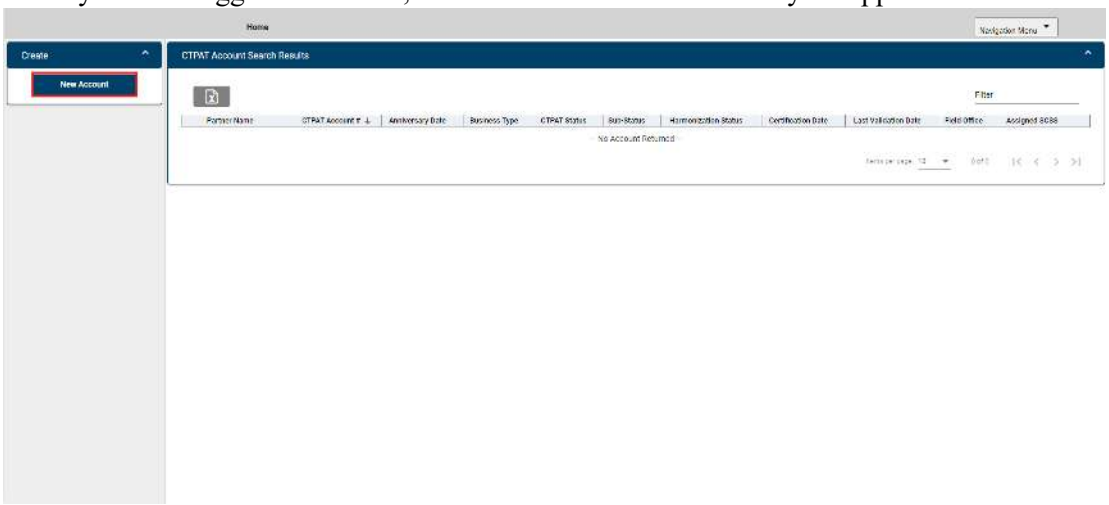
3. Next, click on "Trade/PGA User Login".



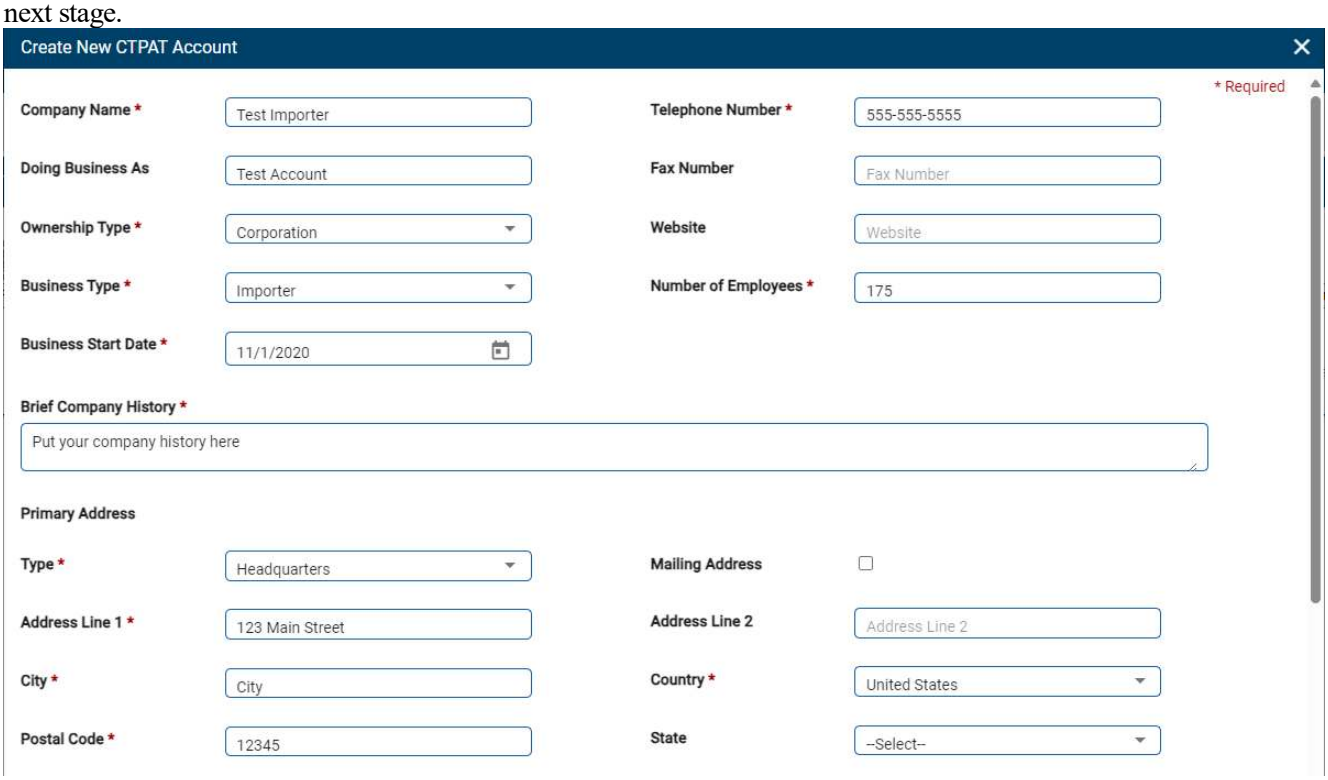
4. Next, you will be directed to log in using the login.gov account you created in step #1. Select the "sign in" button.



5. Once you have logged into Portal, click on “new account” to start your application.



6. Next, fill in all the information. You must complete all the information requested with an asterisk * to progress to the next stage.

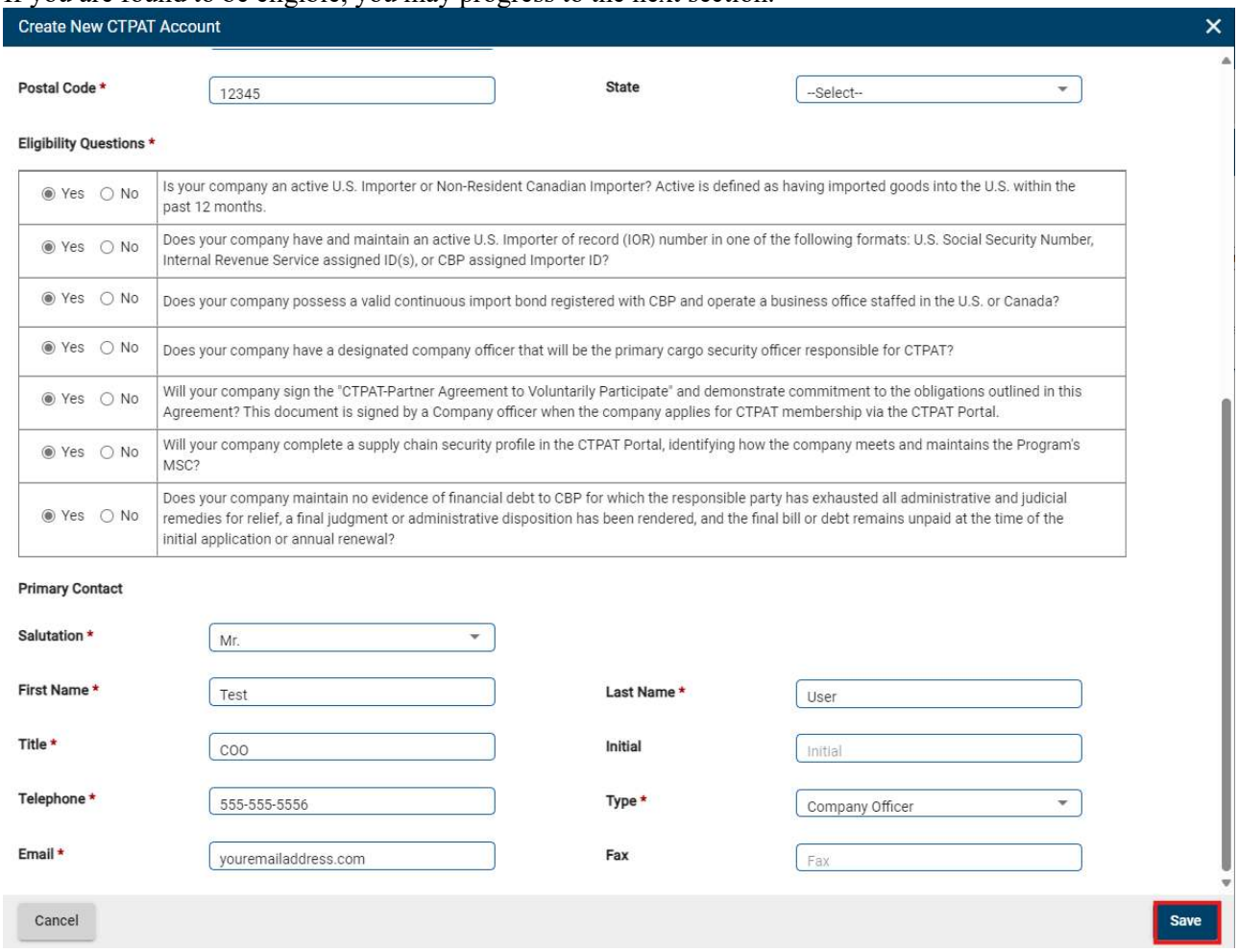


7. Continue filling out all information, including the eligibility questions.

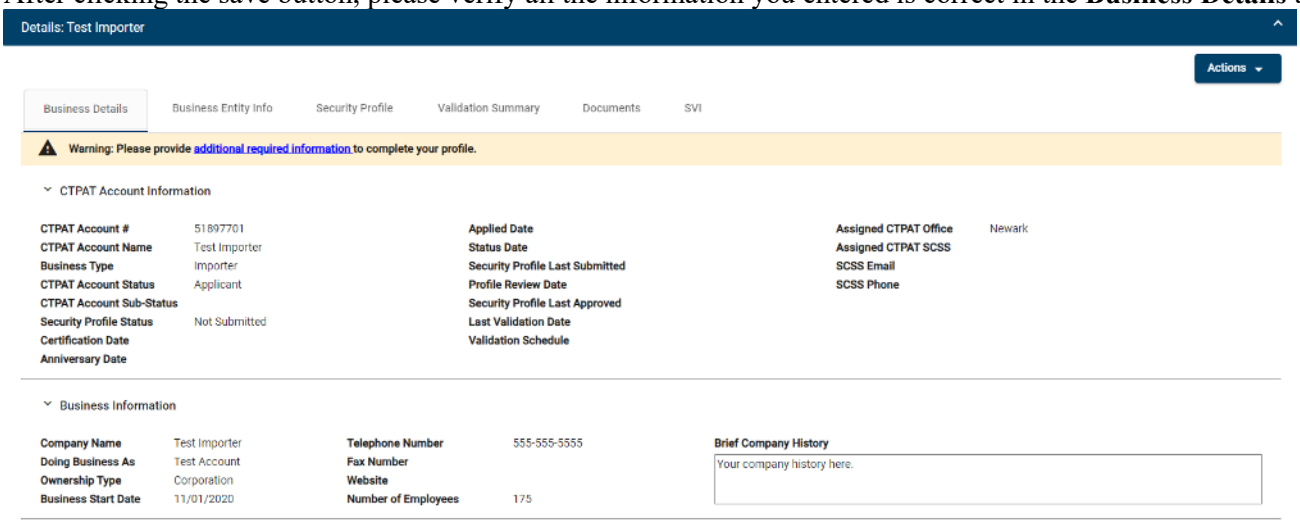
   You must complete all the information requested with an asterisk * to progress to the next stage. When you are done entering the required information, click “save”.

   You cannot proceed without completing this step because this will determine if you are eligible for the program.

   If you are found to be eligible, you may progress to the next section.



8. After clicking the save button, please verify all the information you entered is correct in the **Business Details** tab.



9. Once you verify all the information you entered is correct, add any other addresses, users or Mutual Recognition Arrangements (MRA) with which you would like to share information. Ensure one address is marked as your primary address. Ensure at least one user is marked as primary.

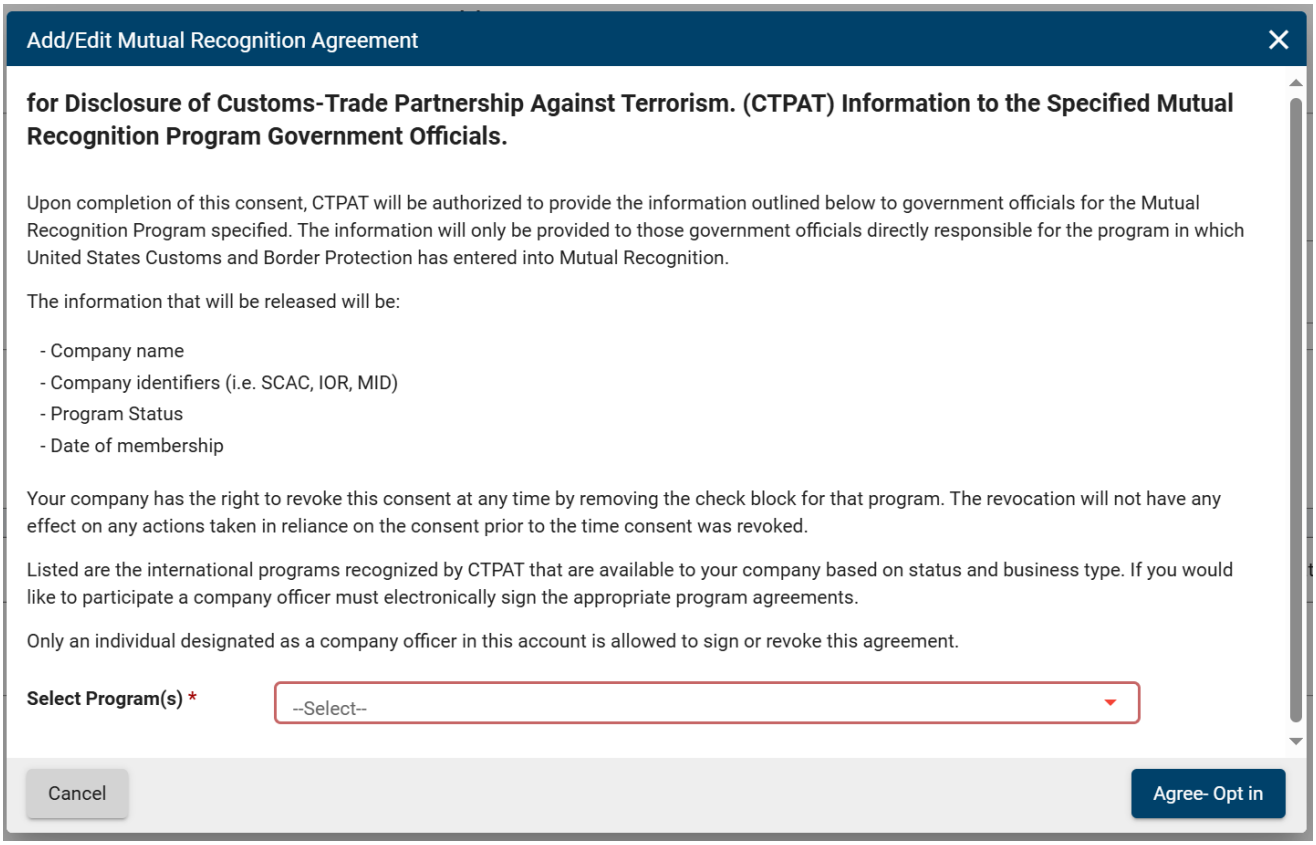
   Every CTPAT account must have a Company Officer. A Company Officer is a person who holds an office of authority and acts in an official capacity on behalf of a company.

   Any contact can update the Security Profile, but only Company Officers can submit the Annual Review and changes to the Security Profile, and electronically sign the CTPAT Partner, Status Verification Interface (SVI), and Mutual Recognition Arrangements.

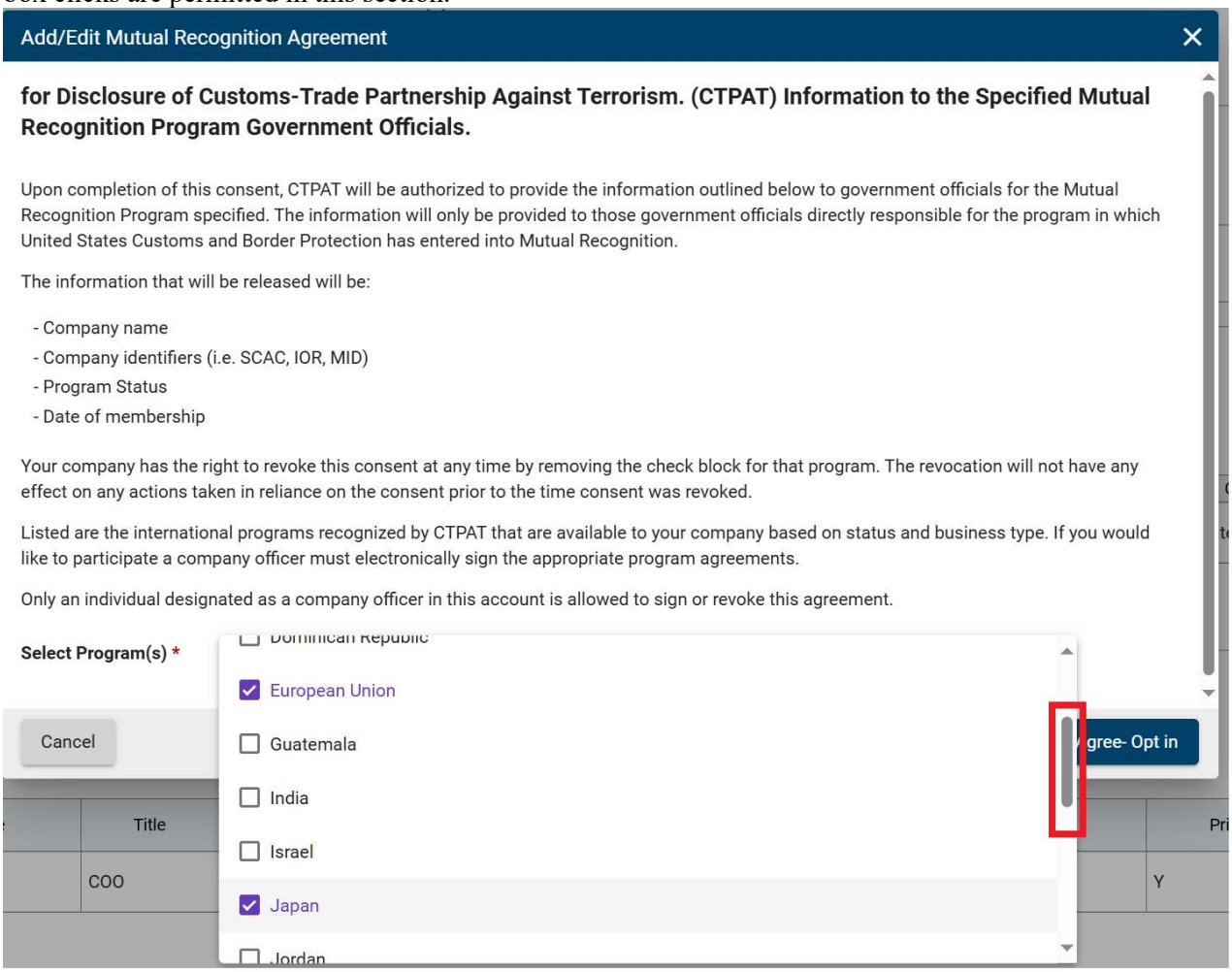
   CTPAT Accounts – User Role Designation things to remember when assigning contact roles:
   - Any contact can update the Security Profile
   - Only a Company Officer can *submit* Security Profile updates to CBP, and sign agreements
   - The Primary POC can be either an Officer or Employee, but not a consultant.



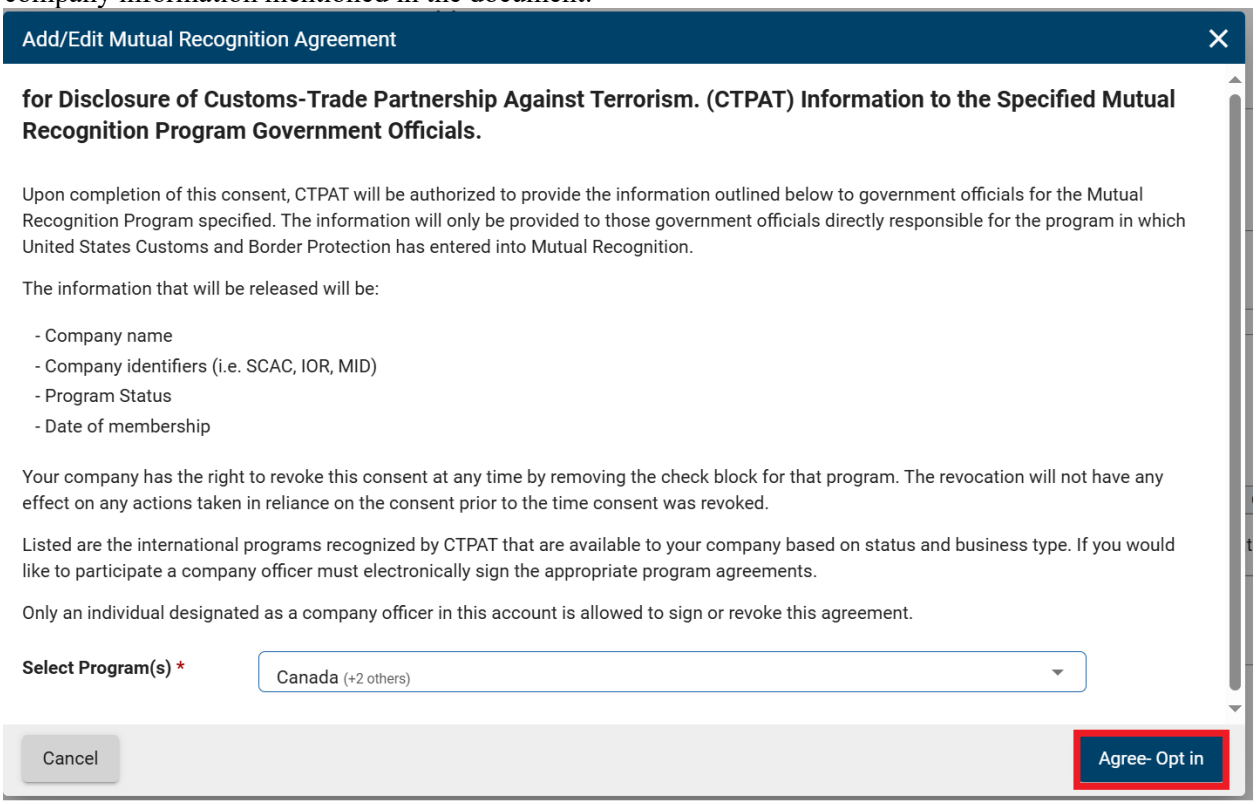
Once you click on the “Add/Edit MR Info.” button, click on the red down arrow to expand the list of programs available.



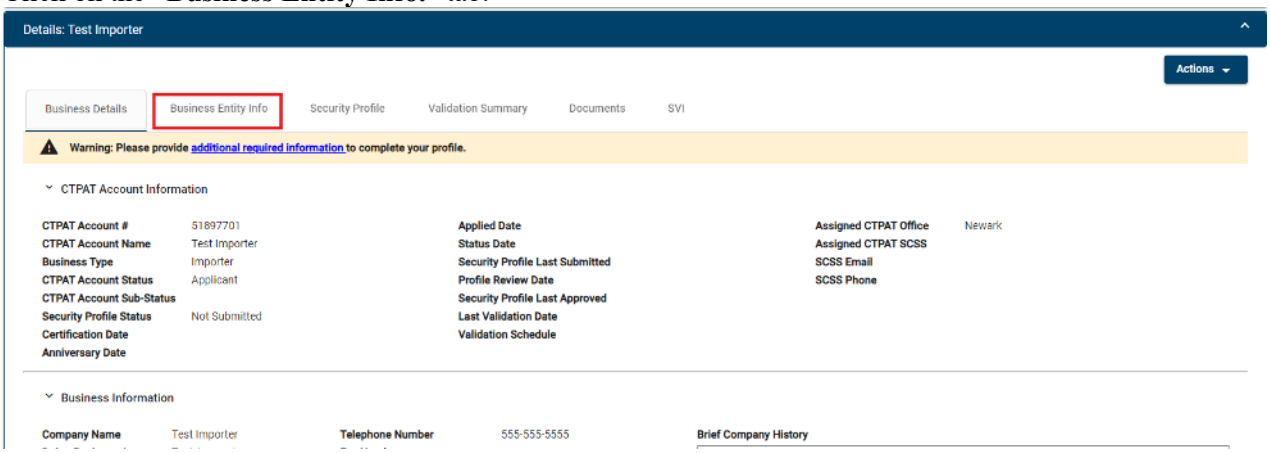
Use the slider to the right of the list to display all available partner countries and click the ones applicable to your company (your company must be exporting/moving cargo to the selected country to receive benefits). Multiple box clicks are permitted in this section.



Then, click the "Agree-Opt in" button. To select any of the MRA partner AEOs, you must agree to sharing company information mentioned in the document.



10. Click on the "**Business Entity Info.**" tab.

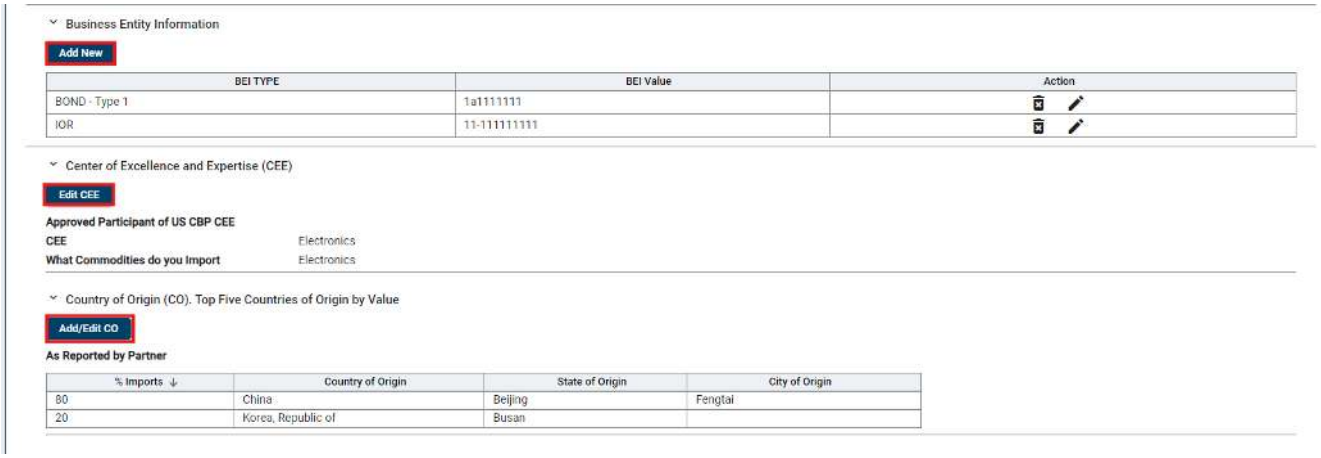


Complete the Business Entity Information (BEI), Centers of Excellence (CEE) and Country of Origin (CO) sections as applicable. The BEIs must be in a specific format to be accepted. Please follow the format in each box or the BEI will not be accepted.

For all business types in CTPAT, certain business entity information is required to be entered as part of the eligibility criteria. For more information on required BEIs, please visit CBP.gov/CTPAT and go to the Applying to CTPAT link on the right.

To enter business identifier information, click "Add New". To delete a business identifier, click the trash can icon on the line of the identifier you wish to delete or the pencil icon to edit.

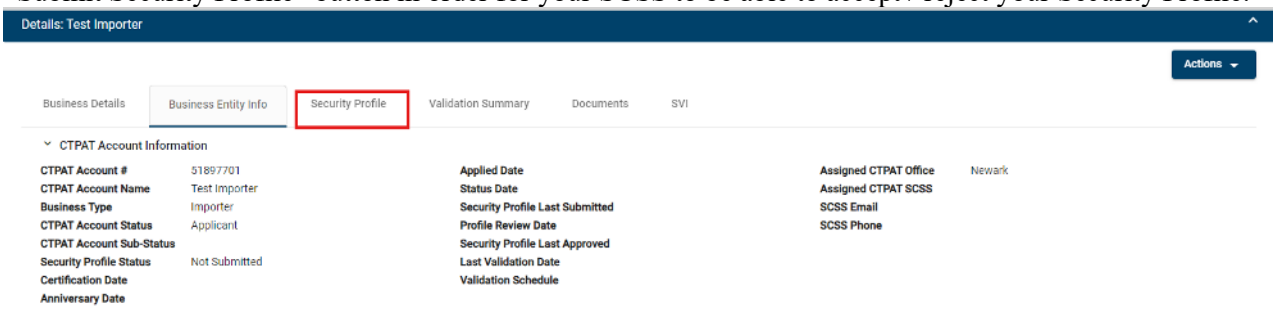
Note: Certain BEIs cannot be added, modified, or removed by Trade Users once they have been entered into your account. Contact your assigned SCSS to add, modify, or remove these BEIs.



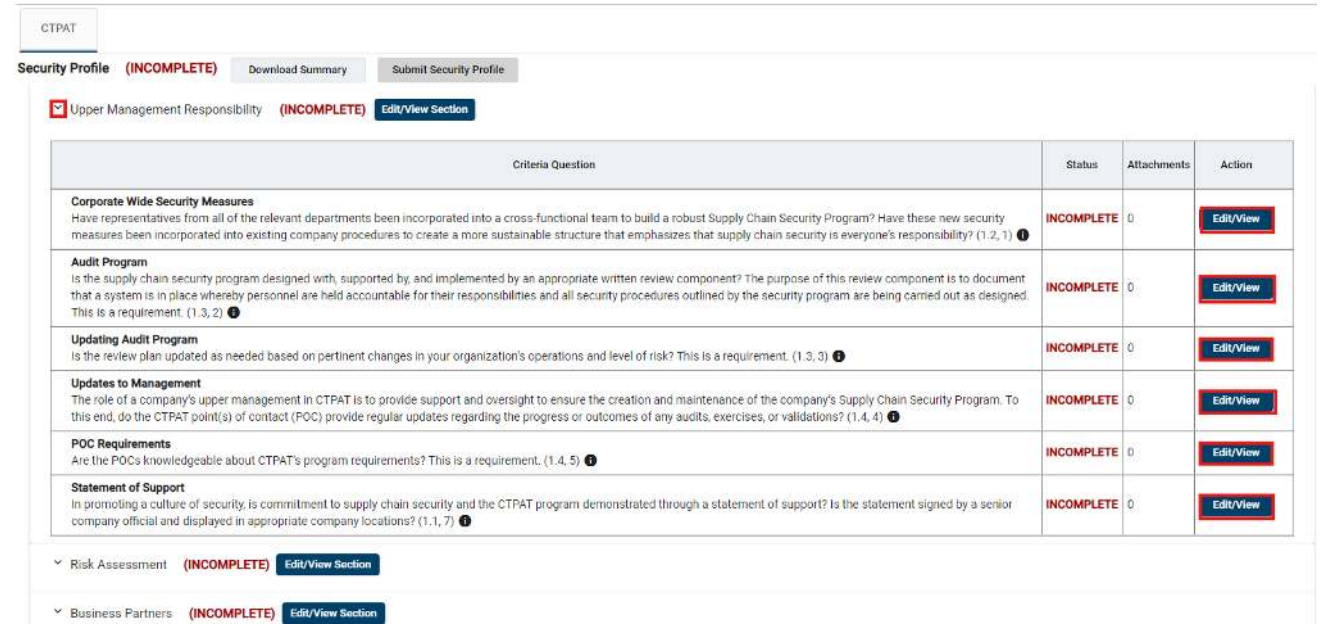
11. Click the "**Security Profile**" tab. The Security Profile is formatted as line-by-line criteria questions that cover the Minimum-Security Criteria listed on CBP.gov/CTPAT. It is recommended that all new applicants review the minimum-security criteria related to the business entity type before starting a CTPAT application.

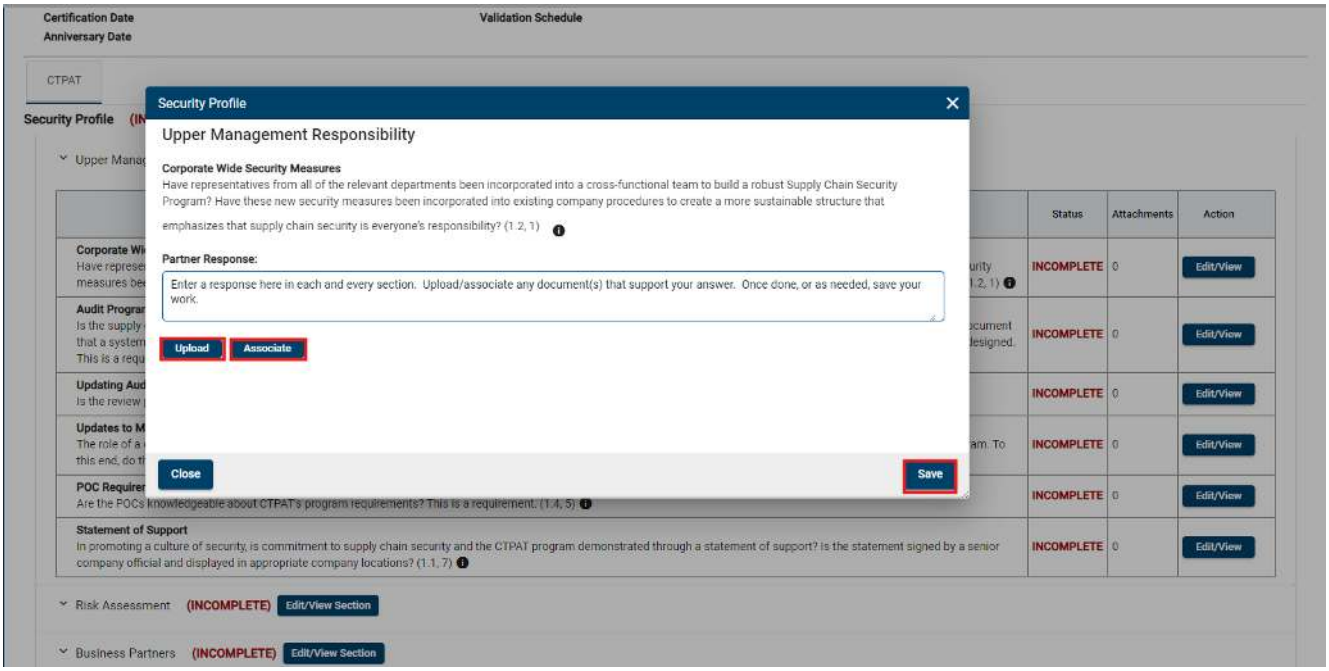
    Answer each criteria question detailing adherence to the security practice or procedure listed in each question. Any evidence the company has of the criteria being implemented must be uploaded; please use the "upload" and "associate" buttons to upload supporting documents. If a question is not applicable to your business model, you may respond "Not Applicable," but must also detail the reason(s) why the statement is not applicable. When data entry is complete, click the "save" button to move to the next question.

    Important! When you have answered all of the Security Profile questions, you MUST click on the "Submit Security Profile" button in order for your SCSS to be able to accept / reject your Security Profile.

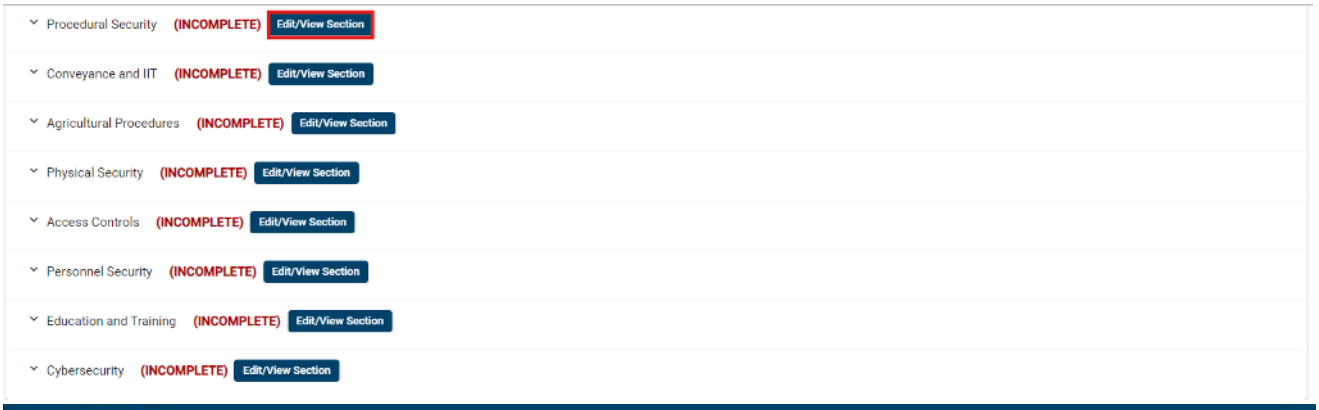


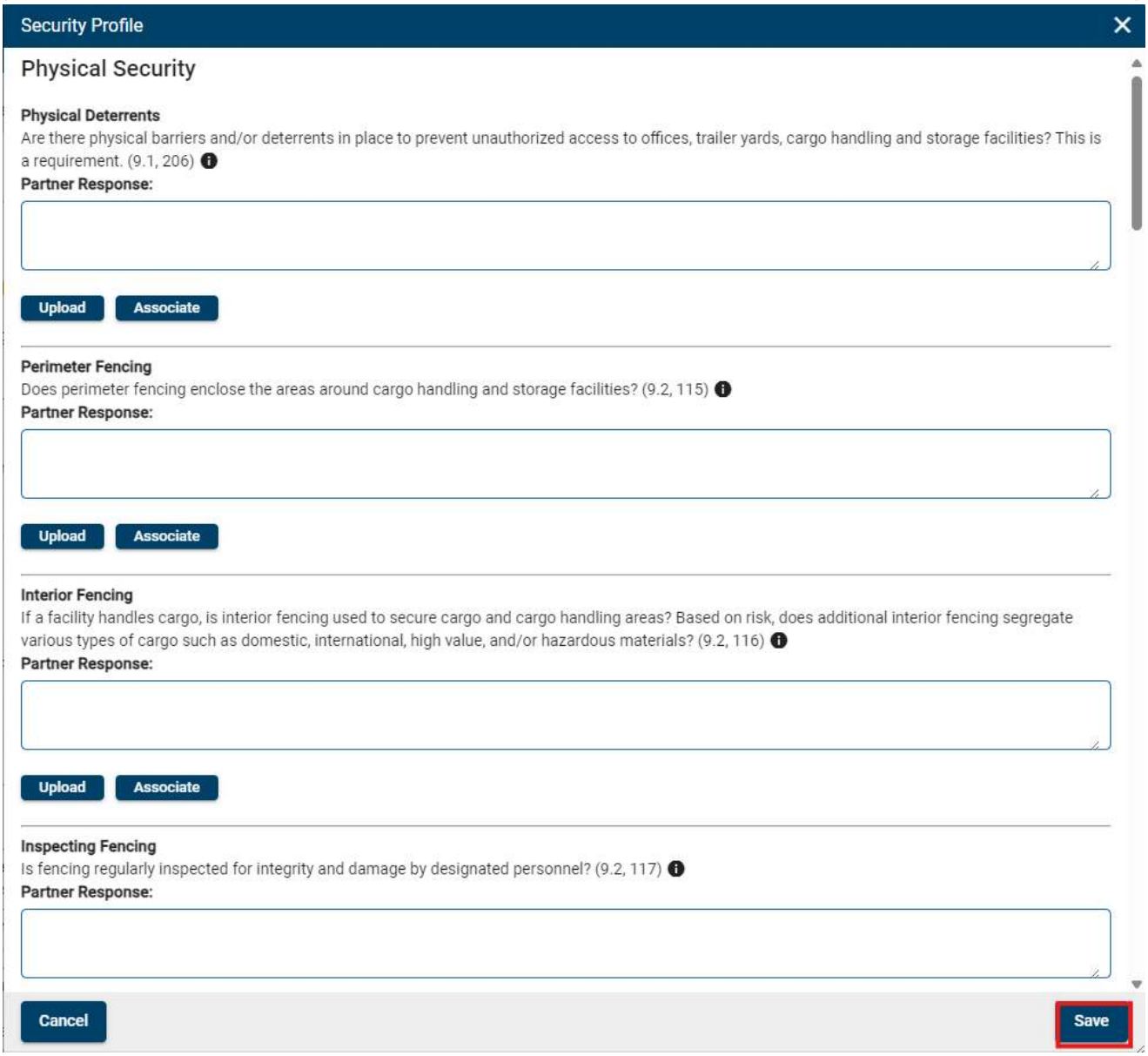
There are two ways you can fill out your Security Profile, you can expand each section and answer every question individually.



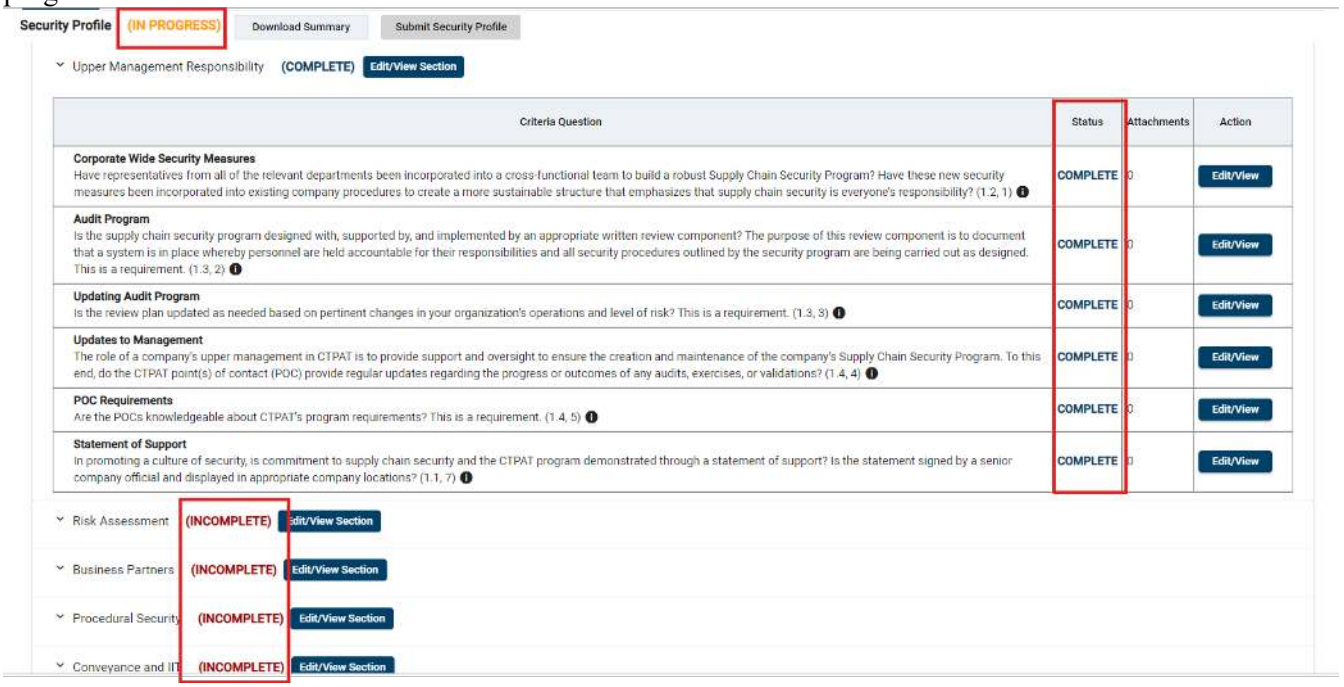


Or you can click “edit/view section”, and all the questions will pop up in a single window. Either way, when done, save your work.





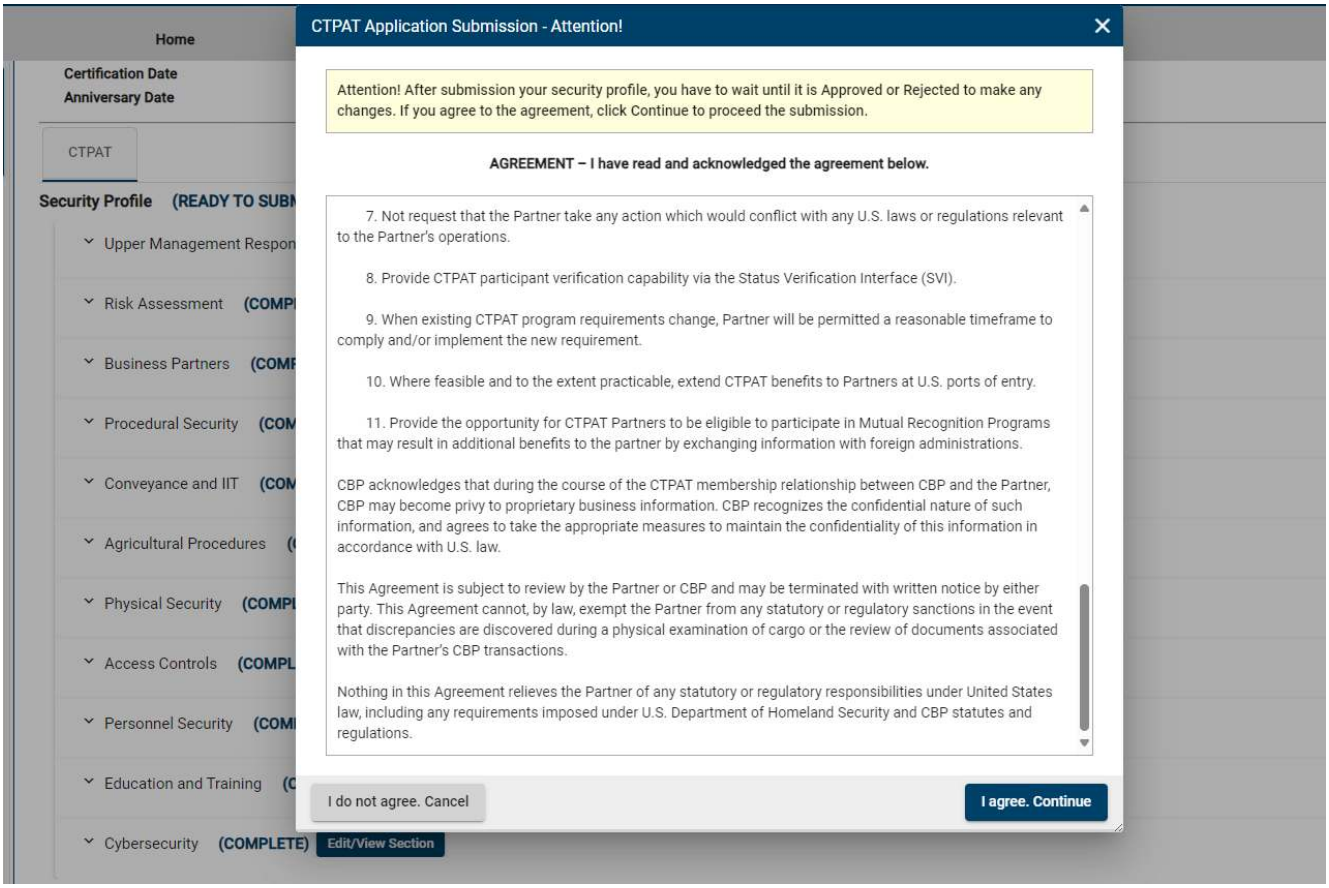
As you complete sections, their status will change to “complete”, and your Security Profile will show as “in progress”.

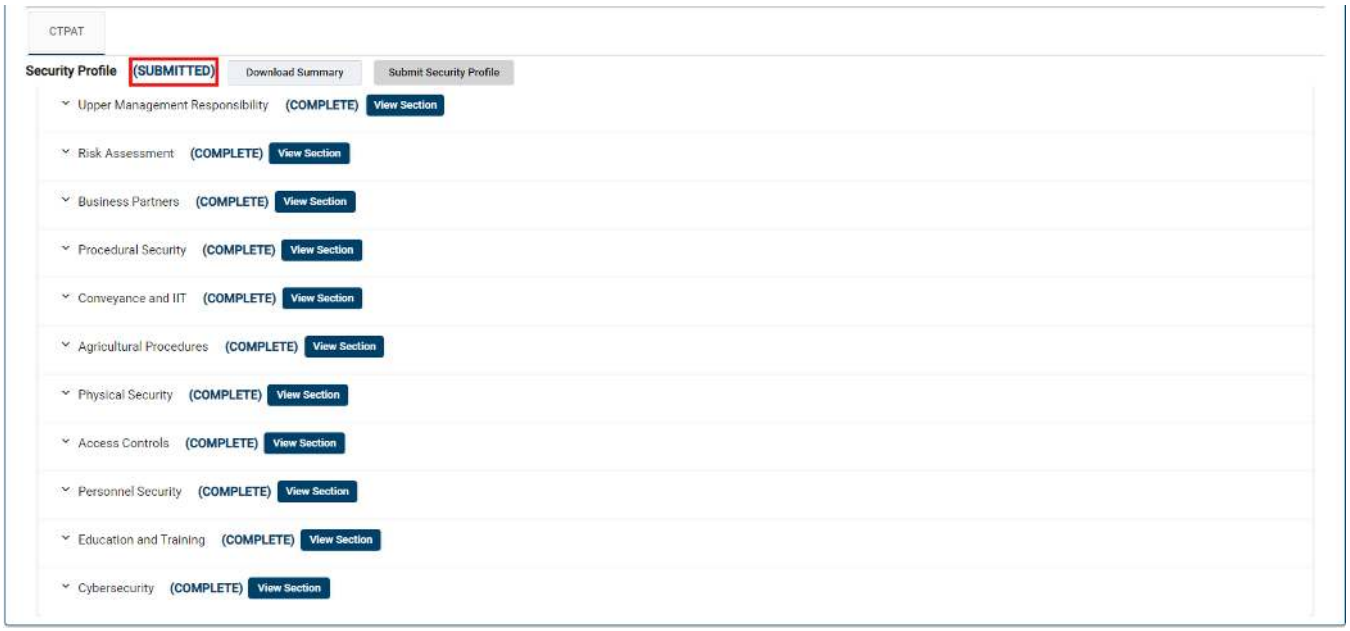


Once you have completed all questions in all sections, your Security Profile status will change to “ready to submit” and you may download a copy before clicking “Submit Security Profile” to submit your application.



Once you submit your Security Profile, you will be asked to electronically sign the user agreement, a copy of this document will automatically be uploaded to your account, and your Security Profile status will update to "submitted".



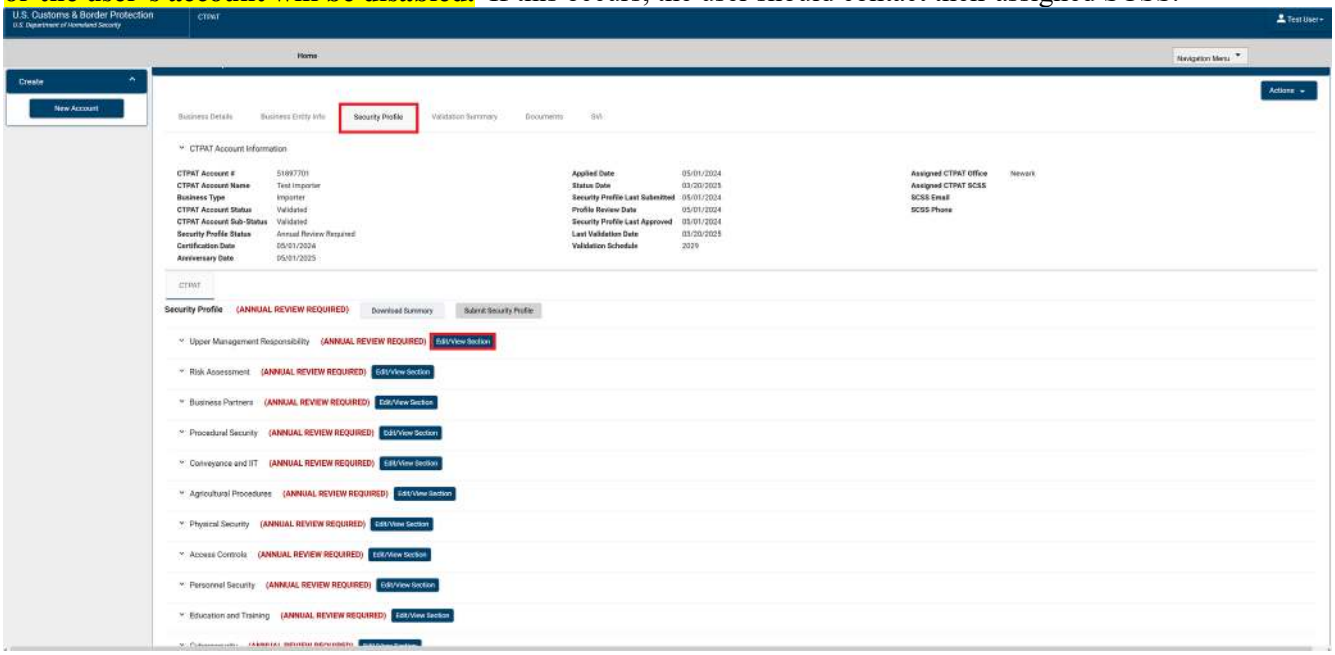


Annual Security Profile review

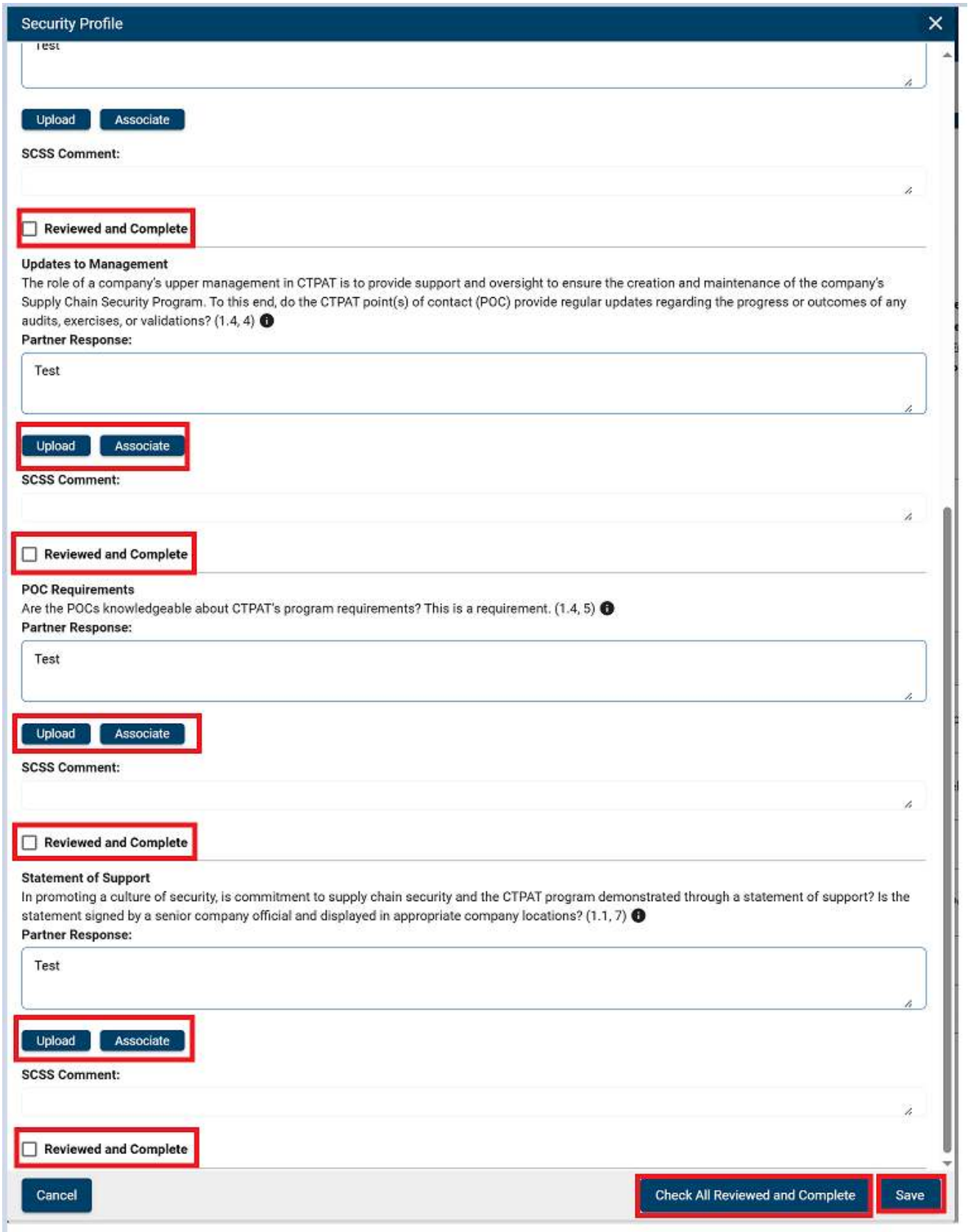
On an annual basis, you must complete the Annual Security Profile review. The Partner Agreement specifies a company agrees to: "complete a supply chain Security Profile and update the Partner's information within that Security Profile on an annual basis". The annual review window is initiated 90 days before the partner anniversary date. While Partners are encouraged to update the Security Profile at any time as company procedures change, only changes made during the 90-day window will satisfy the annual review requirement.

The requirement begins with an annual supply chain risk assessment (guidance to complete a Five Step Risk Assessment can be found at: CTPAT 5-Step Risk Assessment Guide. Completion of the risk assessment may result in changes to your supply chain security policies and procedures. These changes should be reflected in the annual review.

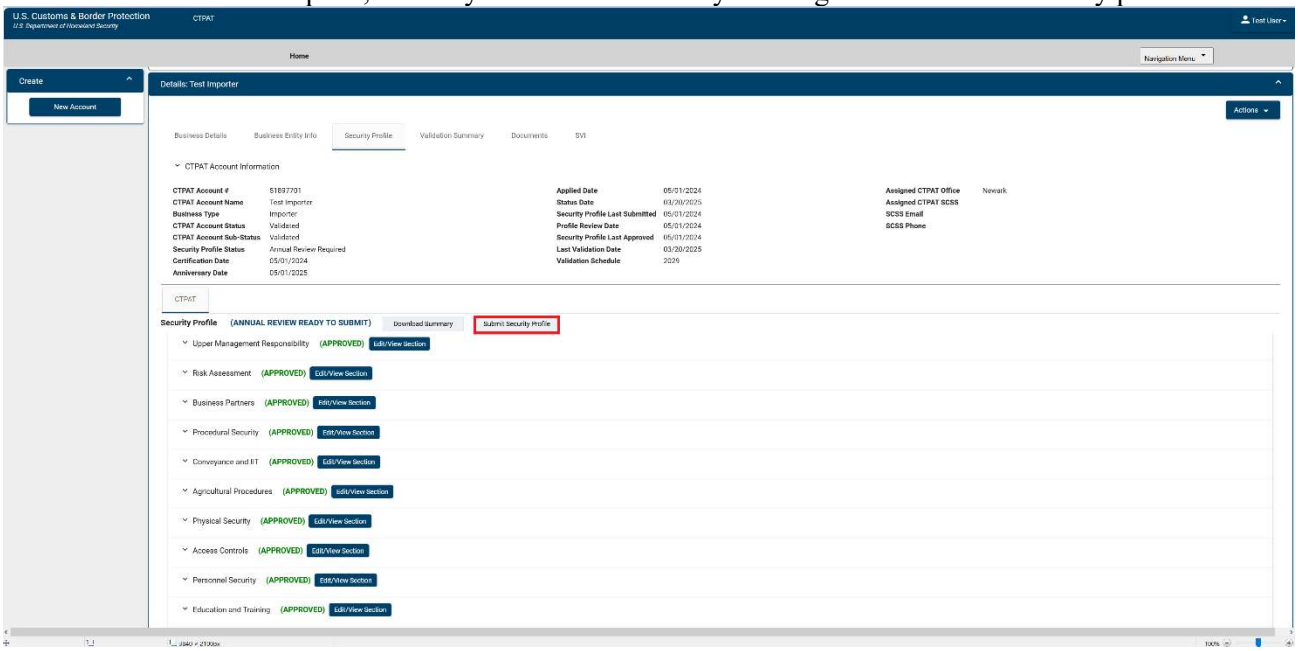
Ninety (90) days prior to the due date the CTPAT Partner account will receive a message with a due date for the annual review. To complete the annual review within the ninety-day window, log into the Partner Portal and navigate to the "**Security Profile**" tab. **Also, each user must log into their Portal account once every 45 days, or the user's account will be disabled.** If this occurs, the user should contact their assigned SCSS.



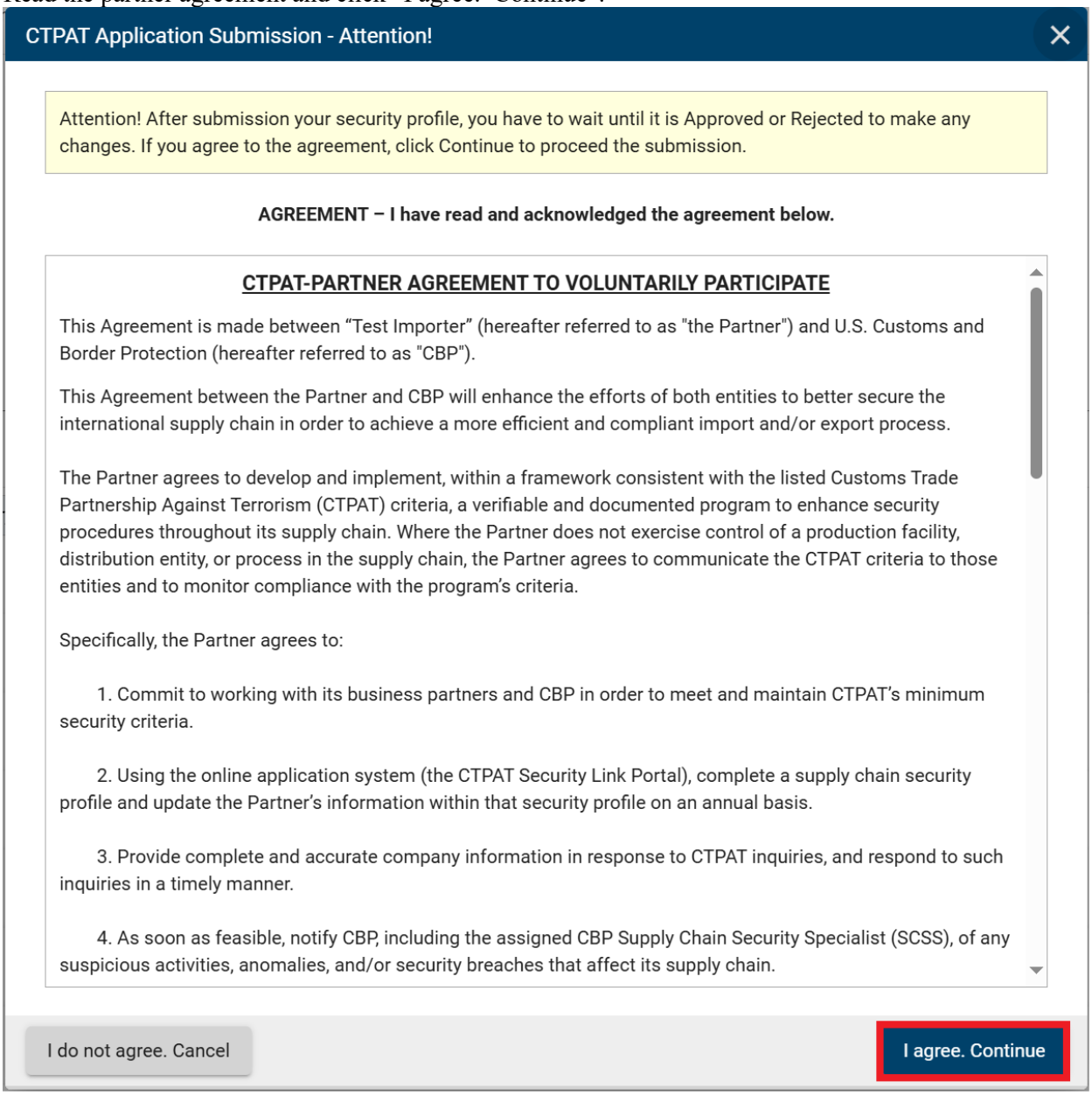
The partner must review all information in the Security Profile. If any updates to security practices and procedures have taken place during the year, update the response to the corresponding criteria statement with the updated information. If no changes in security have taken place, there is no need to add supplemental text. When you agree that the information for an item is correct, check the "reviewed and complete" box and then continue to the next section until all sections have been reviewed and confirmed to be accurate, making any necessary updates as you go.


Security Profile
Test
Upload
Associate
SCSS Comment:
Reviewed and Complete
Updates to Management
The role of a company's upper management in CTPAT is to provide support and oversight to ensure the creation and maintenance of the company's Supply Chain Security Program. To this end, do the CTPAT point(s) of contact (POC) provide regular updates regarding the progress or outcomes of any audits, exercises, or validations? (1.4, 4)
Partner Response:
Test
Upload
Associate
SCSS Comment:
Reviewed and Complete
POC Requirements
Are the POCs knowledgeable about CTPAT's program requirements? This is a requirement. (1.4, 5)
Partner Response:
Test
Upload
Associate
SCSS Comment:
Reviewed and Complete
Statement of Support
In promoting a culture of security, is commitment to supply chain security and the CTPAT program demonstrated through a statement of support? Is the statement signed by a senior company official and displayed in appropriate company locations? (1.1, 7)
Partner Response:
Test
Upload
Associate
SCSS Comment:
Reviewed and Complete
Cancel
Check All Reviewed and Complete
Save

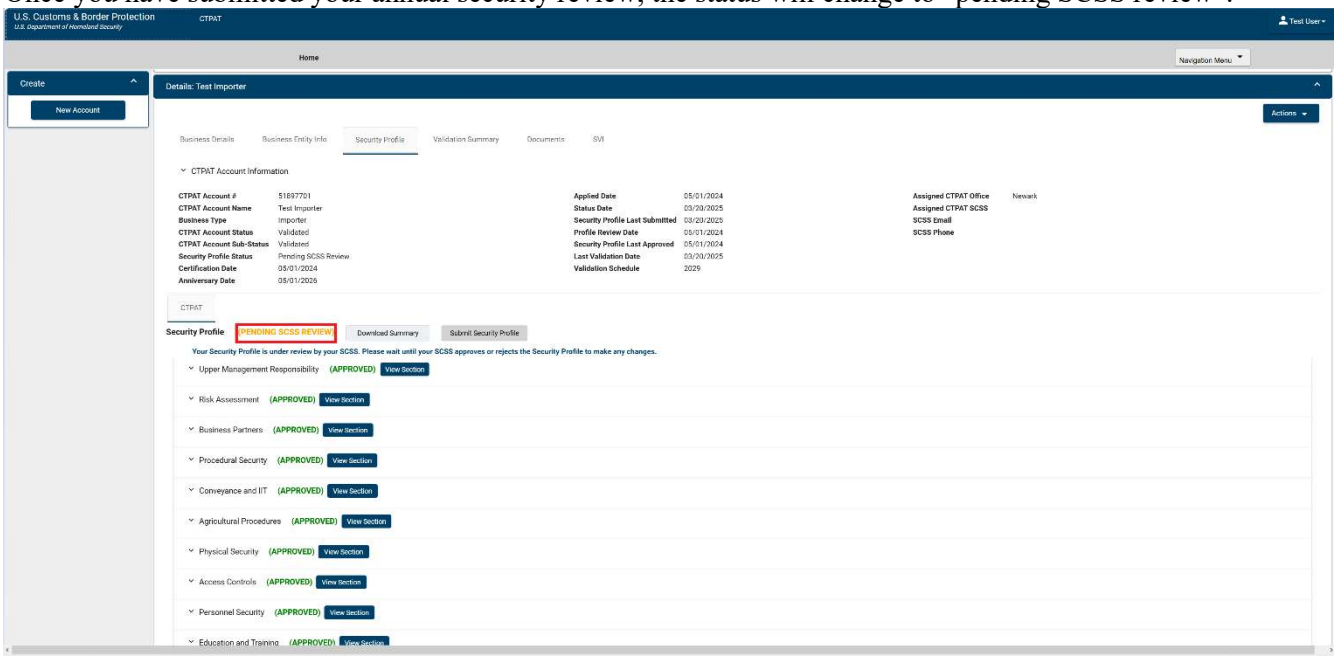
Once all sections are complete, submit your annual review by clicking on the “submit security profile” button.



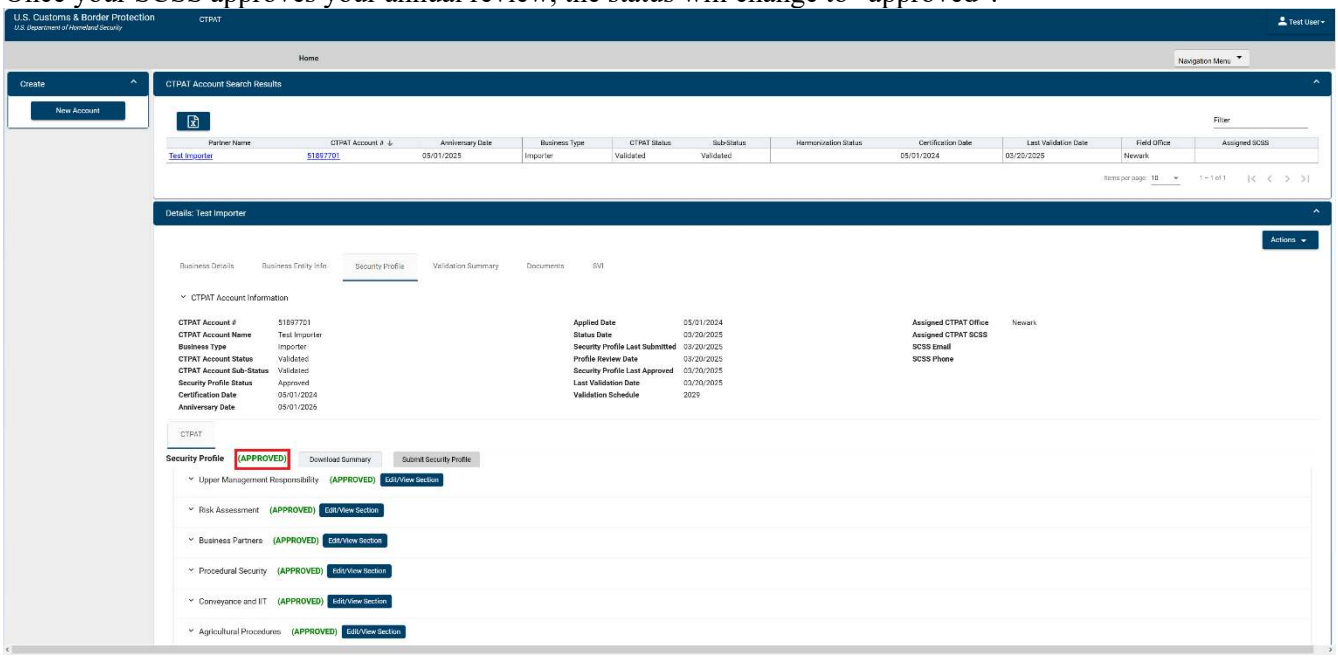
Read the partner agreement and click “I agree. Continue”.



Once you have submitted your annual security review, the status will change to “pending SCSS review”.

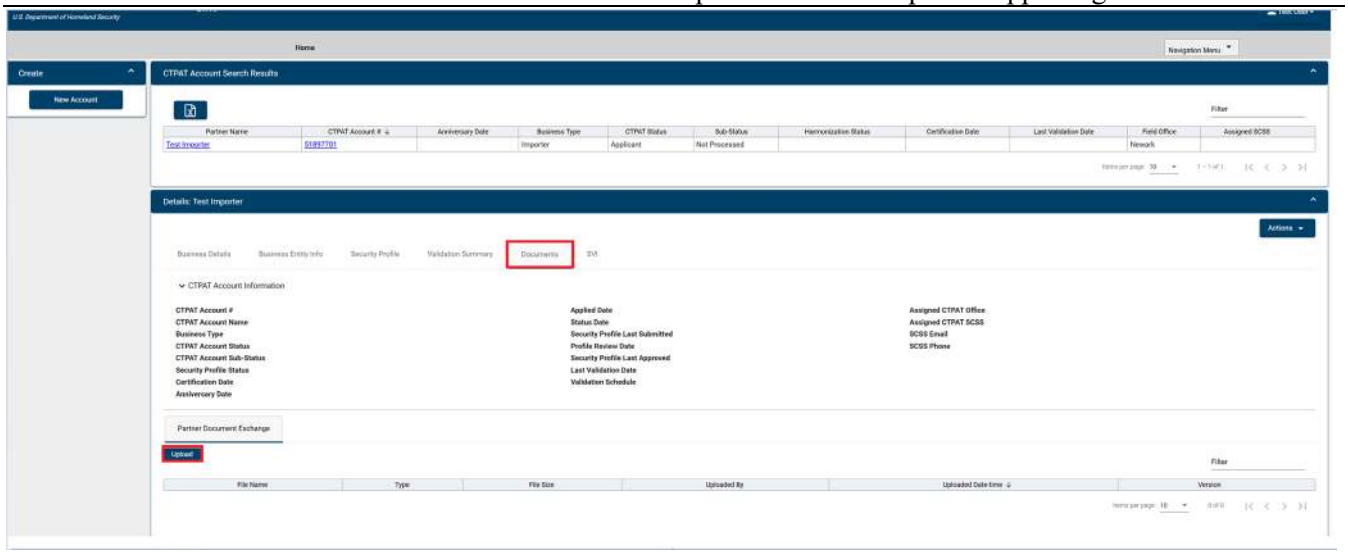


Once your SCSS approves your annual review, the status will change to “approved”.

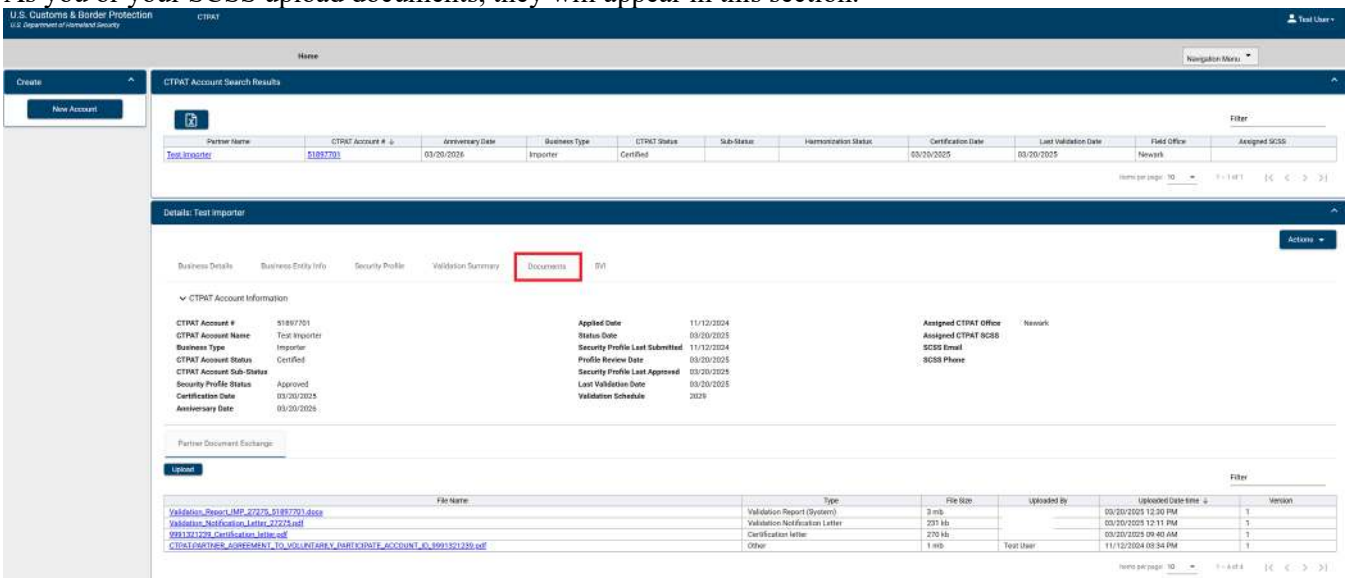


Documents

OPTIONAL: Click on the "**documents**" tab. Click the "upload" button to upload supporting documents.



As you or your SCSS upload documents, they will appear in this section.



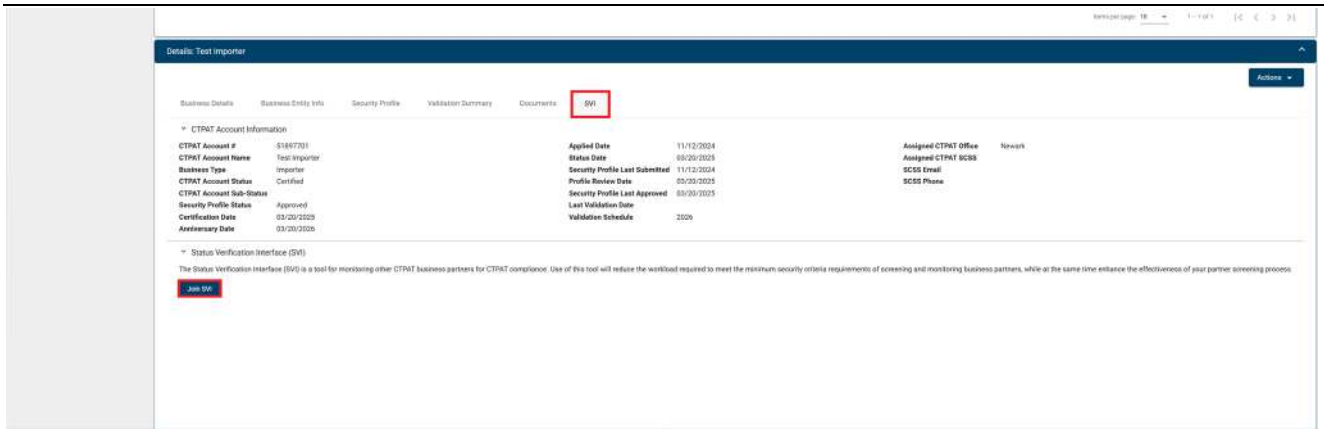
Status Verification Interface (SVI)

SVI Partner monitoring allows CTPAT Partners to track the CTPAT status of their business partners.

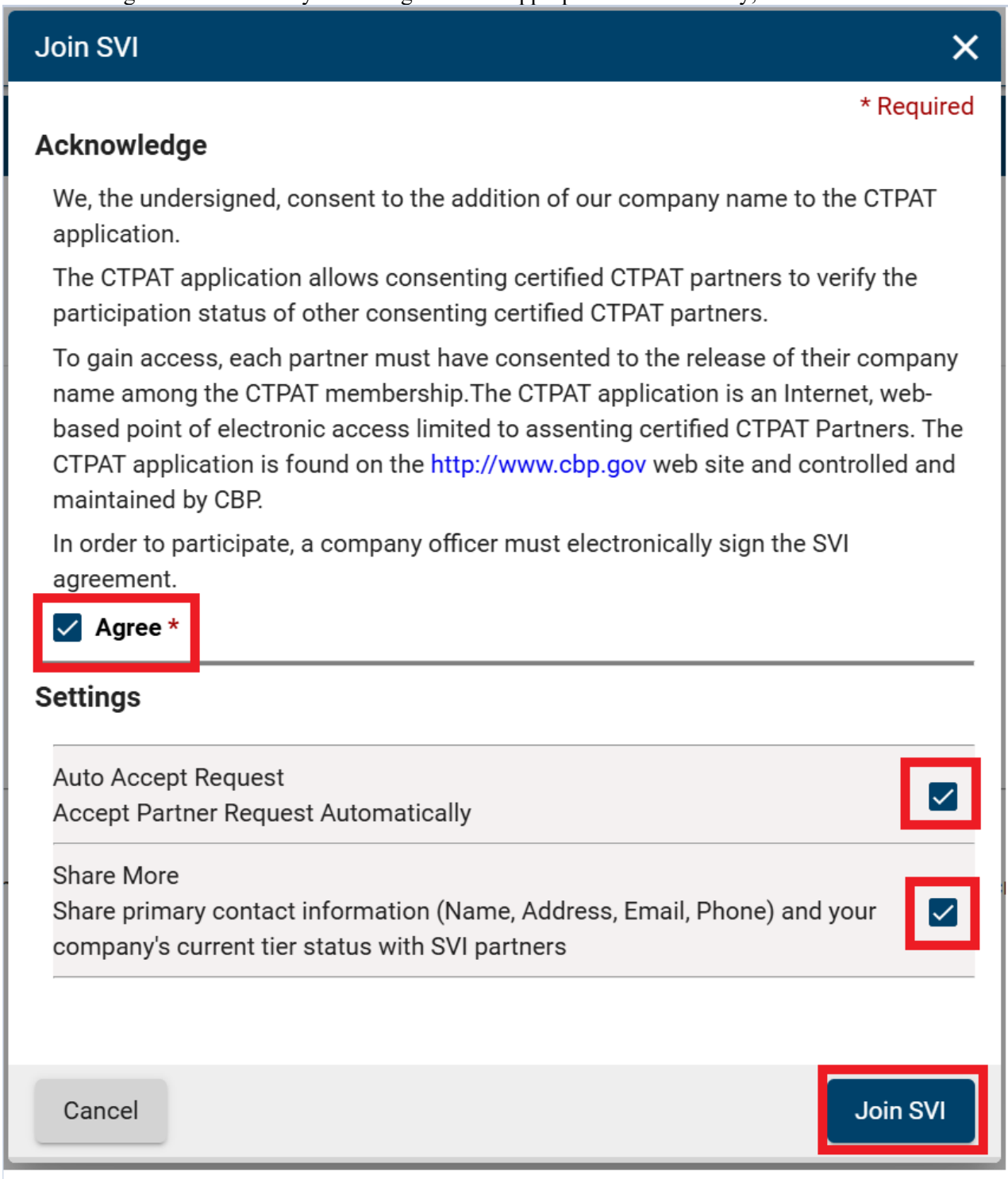
SVI Requirements
To participate in SVI, a company must:

(1) Have a Certified CTPAT account in good standing.
(2) Consent to share your status with other companies, as is stated in the SVI Agreement. *NOTE: If SVI agreement is revoked, your company will be removed from all Partners Monitoring You and all Partners You are Monitoring.*

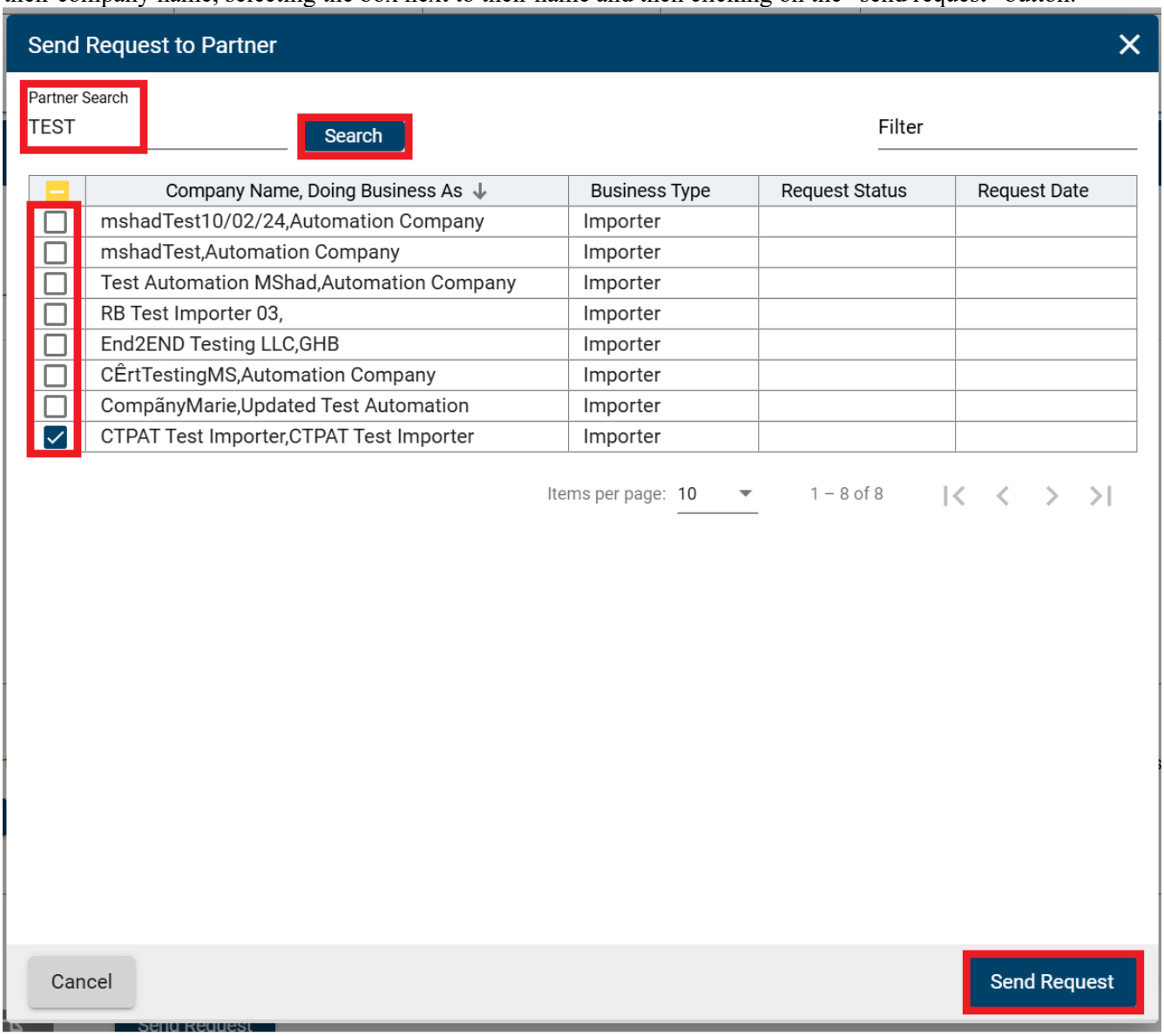
Click on the "**SVI**" tab. Then click "Join SVI".



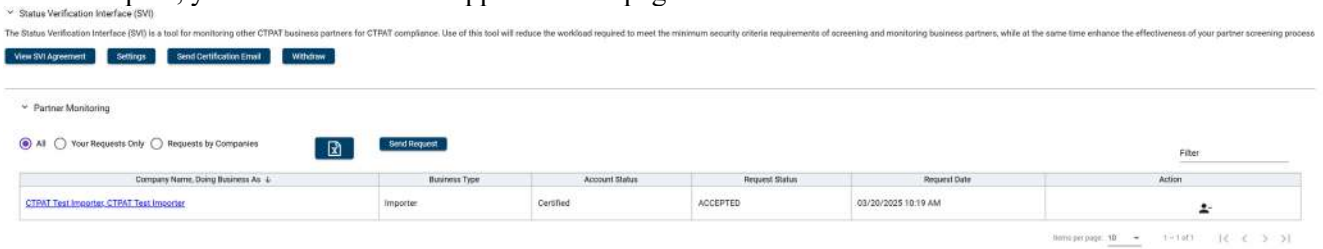
Check the “agree” box. Choose your setting and click appropriate boxes. Lastly, click “Join SVI”.



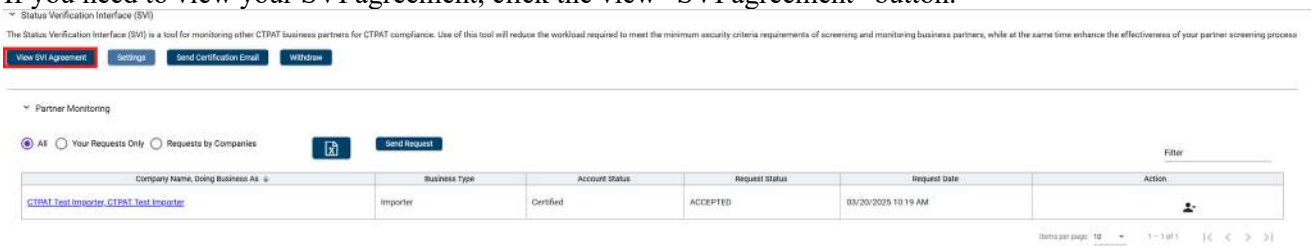
You may now search for your partners and send them requests via the SVI system. This is done by searching for their company name, selecting the box next to their name and then clicking on the “send request” button.



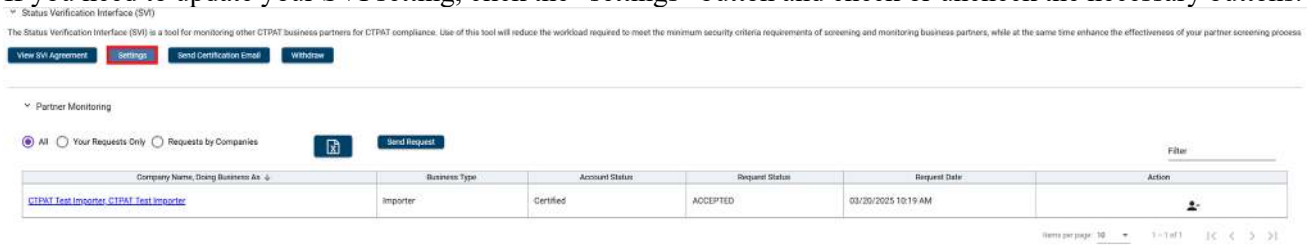
Once accepted, your connections will appear on this page.

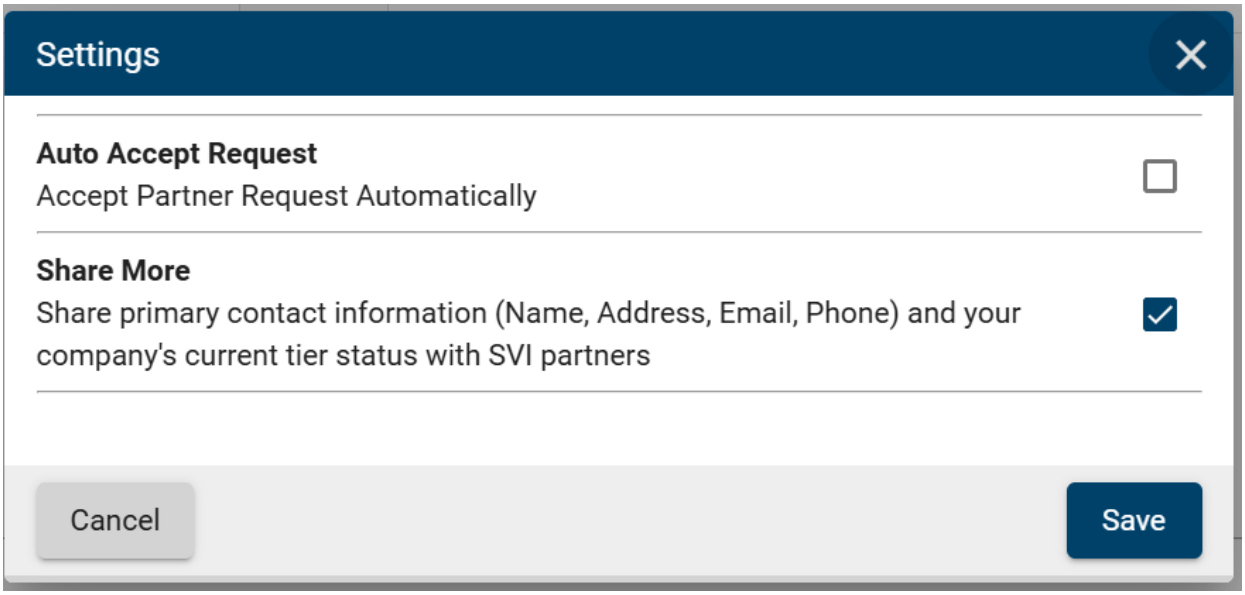


If you need to view your SVI agreement, click the view “SVI agreement” button.

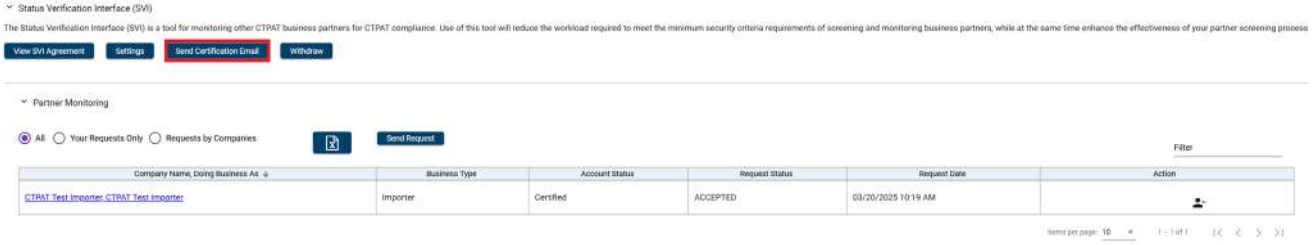


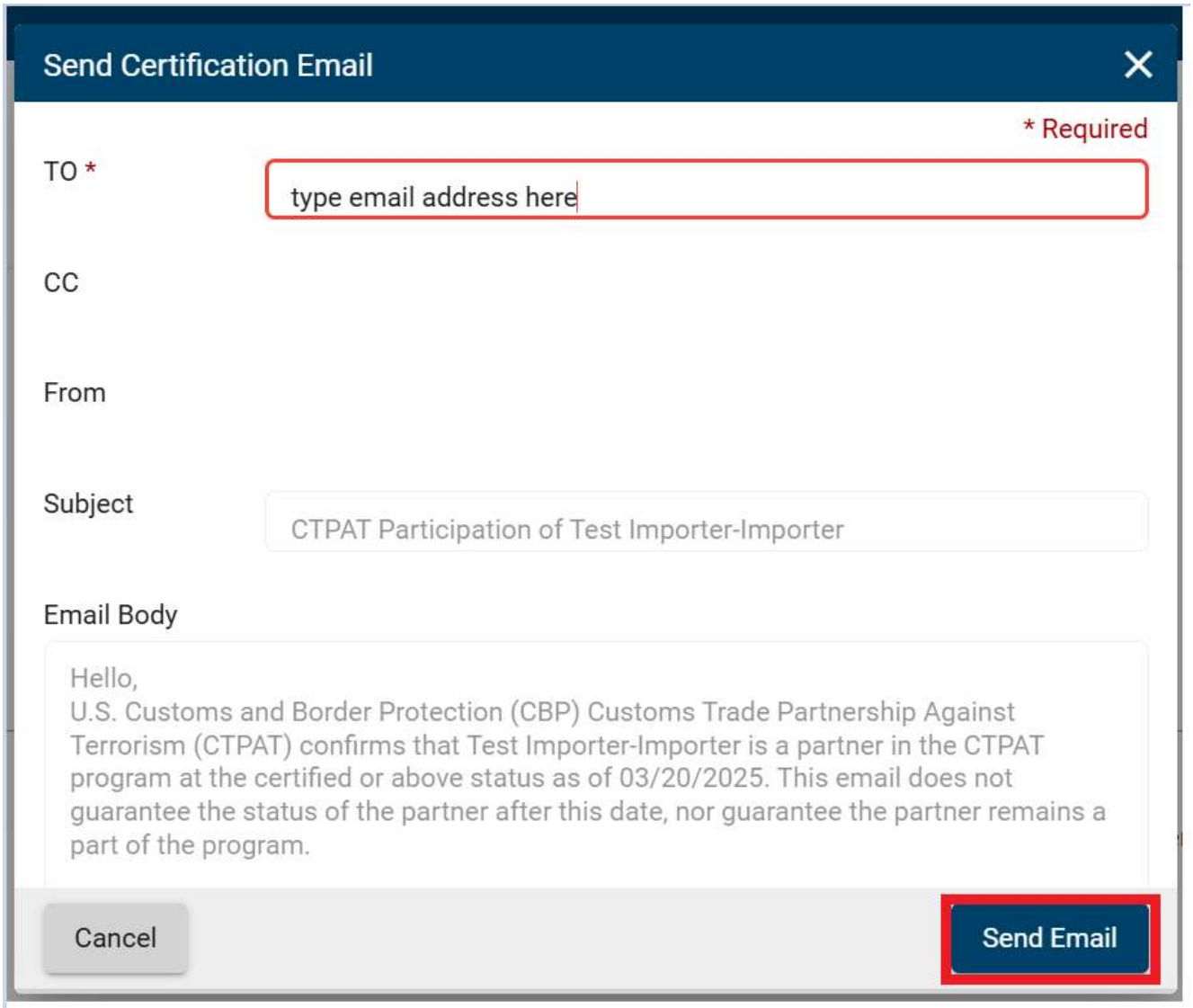
If you need to update your SVI setting, click the “settings” button and check or uncheck the necessary buttons.



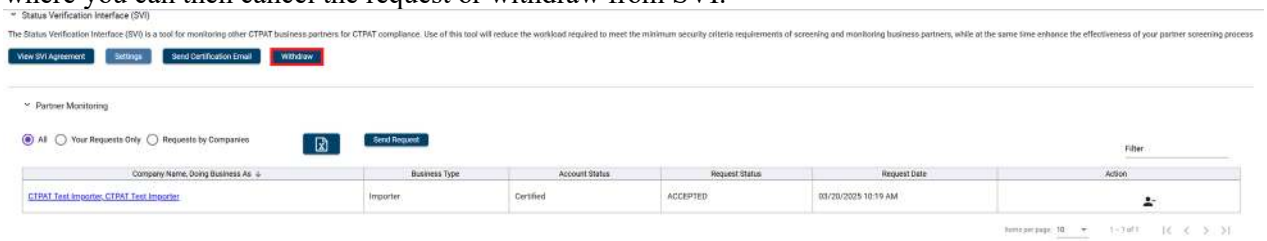


If you need to send an email confirming that you are a certified CTPAT partner, you can do so by clicking the "send confirmation" email button and then filling out the email address and pressing the "send email" button.



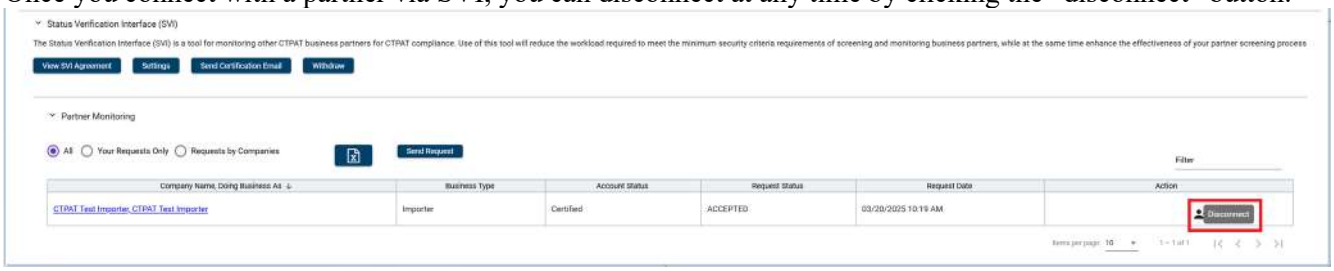


If you decide to withdraw from the SVI program, click the “withdraw” button. A pop-up window will appear where you can then cancel the request or withdraw from SVI.

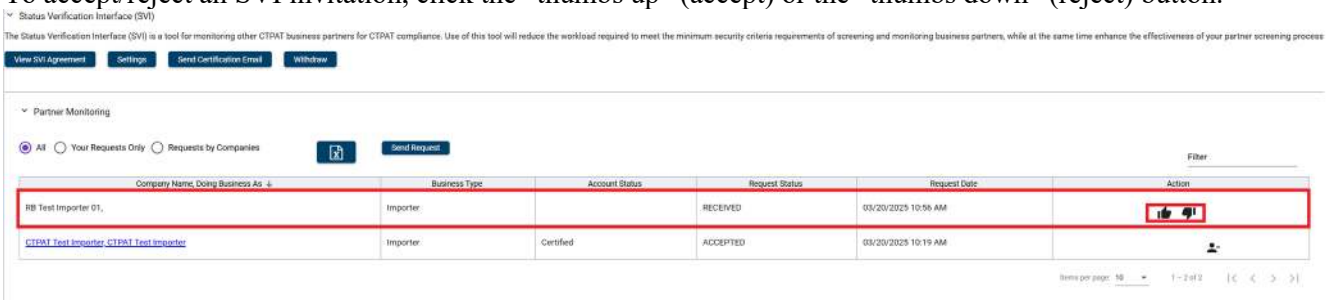




Once you connect with a partner via SVI, you can disconnect at any time by clicking the “disconnect” button.

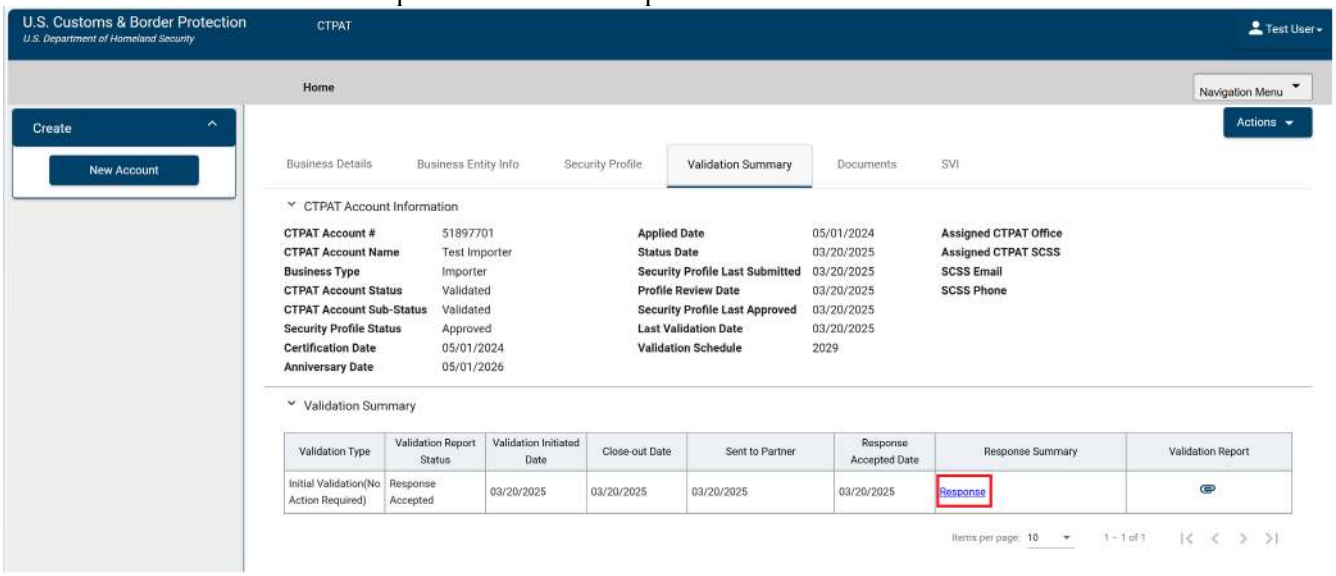


To accept/reject an SVI invitation, click the “thumbs up” (accept) or the “thumbs down” (reject) button.

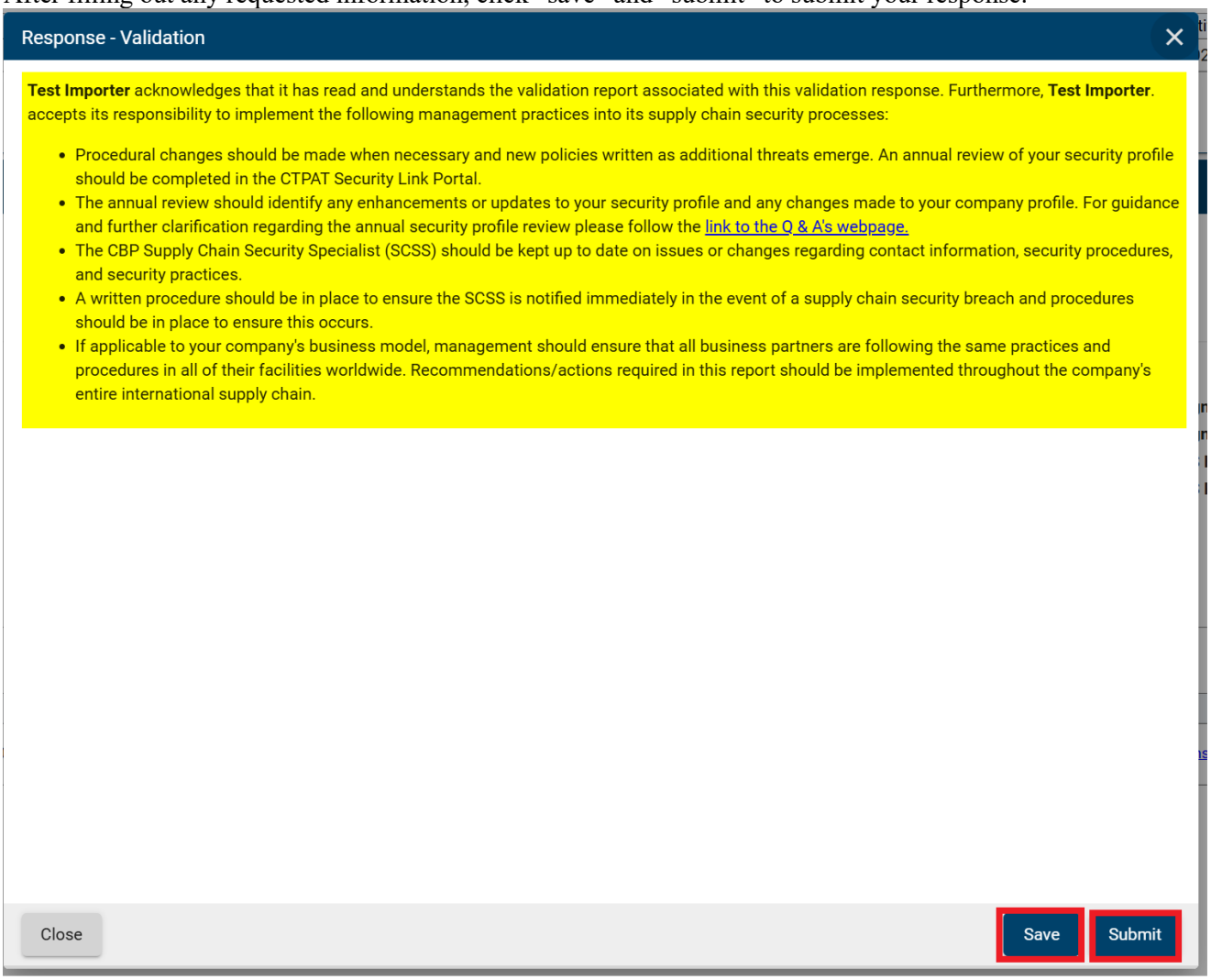


Validation

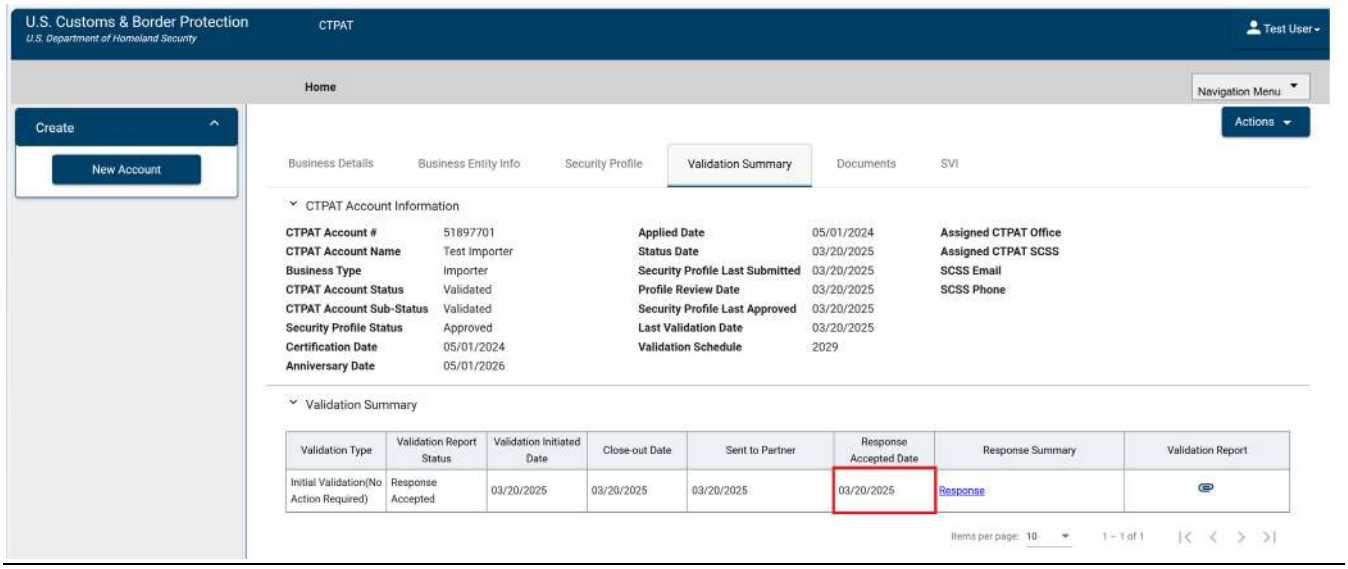
Click on the “**Validation Summary**” tab. Once completed, your validation report is available in the lower window for each validation that has been completed for your company. See “Validation Report” block below. Click on the desired validation report to see more details. As a partner, you must complete your validation response. See “Response Summary” block below. To do so, click on the “response” button. Use the space provided in the text boxes to reply to the Recommendations or Actions Required listed and use the upload button under each text box to include required evidence of implementation.



After filling out any requested information, click “save” and “submit” to submit your response.

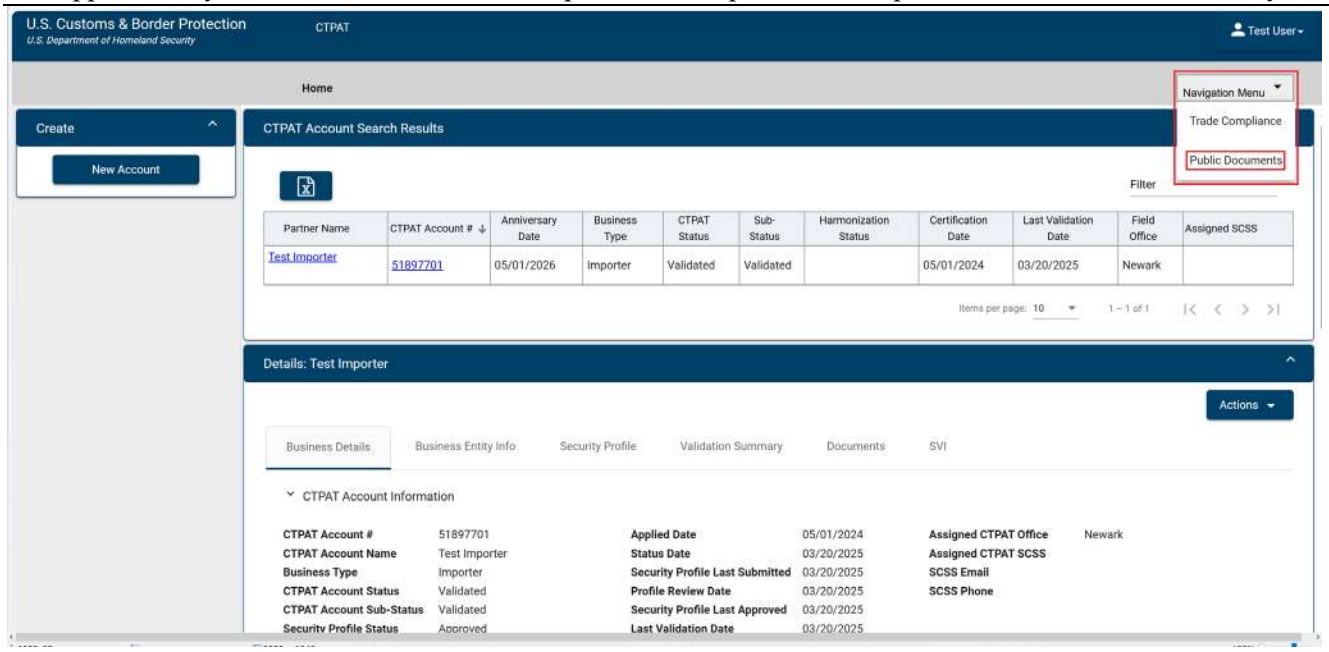


Once your SCSS has reviewed and approved your response, a date will appear in the response accepted date field.

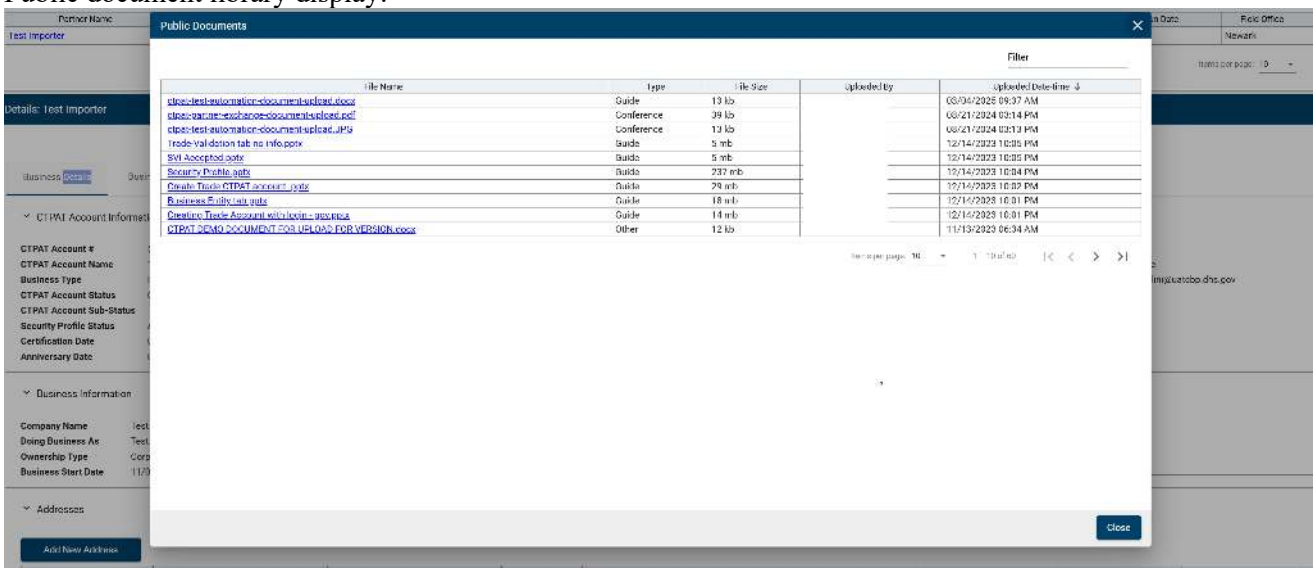


Public Document Library

All users in an account will have access to documents in the Public Document Library. To access the Public Document Library, click the navigation menu and then click on “public documents”. All available documents will appear. Only CBP CTPAT administrative personnel are permitted to upload documents into this library.

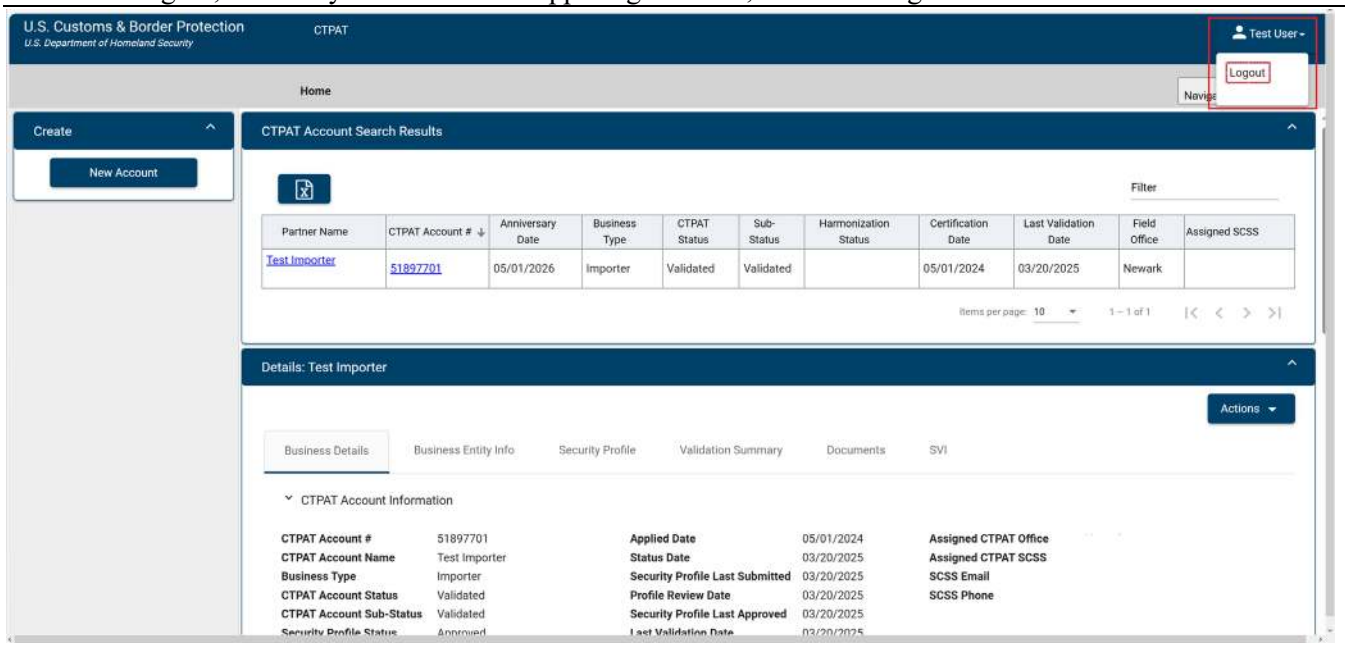


Public document library display:



Logout

In order to logout, click on your name in the upper right corner, and select logout.



Troubleshooting

For issues or questions while applying to CTPAT, please contact your closest CTPAT filed office:

- Buffalo, New York ctpatfieldofficebuffalo@cbp.dhs.gov
- Houston, Texas ctpatfieldofficehouston@cbp.dhs.gov
- Laredo, Texas ctpatfieldofficelaredo@cbp.dhs.gov
- Los Angeles, California ctpatfieldofficelosangeles@cbp.dhs.gov
- Miami, Florida ctpatfieldofficemiami@cbp.dhs.gov
- New York, New York ctpatfieldofficenewyork@cbp.dhs.gov
- Newark, New Jersey ctpatfieldofficenewark@cbp.dhs.gov

You may also contact the CTPAT Headquarters Office located in Washington, D.C.

- Washington, D.C. OFO-INDUSTRYPARTNERSHIP@cbp.dhs.gov

Note: Technical issues should be reported via telephone to the national Help Desk at 1-800-927-8729 or via email to ctpathelpdesk@cbp.dhs.gov.

Publication Number 5009-0425