



Trading Partner Manager (TPM) & Onboarding Module (OBM) User Guide

March 2024

A decorative background consisting of several intersecting lines in red and grey, creating a dynamic, geometric pattern.

EXOSTAR[®]



CONTENTS

Document Versions	3
Guide Overview	4
Step 1: Login to Exostar’s Managed Access Gateway (MAG)	4
Step 2: Access Trading Partner Manager (TPM)	5
Step 3: Update Cyber Security Section of Self Certification	6
Step 4: Complete the Cybersecurity Compliance Risk Assessment (CCRA) Questionnaire	9
Submitter’s Details Page Guidance.....	16
Update Completed Form	17
Form Upgrade.....	17
Form Grouping.....	18
Business Issue	18
Solution	19
Group Setup.....	19
View Form Groups	20
Onboarding Module Resources	20



DOCUMENT VERSIONS

Version	Change Overview	Date	Responsible Party
1	Formatting and Release Updates (Previously TPM PIM Guide)	March 2024	Ashleigh Howell



GUIDE OVERVIEW

This guide provides instructions to update your organization's cybersecurity posture within Trading Partner Management (TPM) and Onboarding Module (OBM), as well as the following organization maintenance processes:

- Performing general organization TPM maintenance. This can be performed when your organization's status is either Active or Expired.
- Completing the CCRA questionnaire in OBM, which is necessary for Lockheed Martin to make risk- based procurement decisions of your company's products and services.

IMPORTANT: Only the Organization Administrator, having logged in with 2-Factor Authentication (2FA) credentials, can make changes to the company's TPM profile. For more information on 2FA credentials please visit https://www.myexostar.com/?ht_kb=lockheed-martin#lockheed-martin-accepted-credentials.

It is also important to note, to recertify an organization, there must be at least one (1) active LMP2P user with 2FA credentials (this can be the Organization Administrator) associated with the organization.

STEP 1: LOGIN TO EXOSTAR'S MANAGED ACCESS GATEWAY (MAG)

To access your TPM profile, you must first login to your Exostar's Managed Access Gateway (MAG) account. For help resetting your MAG password or any other MAG-related questions, refer to https://www.myexostar.com/?ht_kb=mag.

NOTE: If you are the first user in your organization to access OBM, you must accept the standard MAG Usage Service Agreement. If you see **Agree to Terms** on the **Onboarding Module** tile in your MAG account, click the button and accept the service agreement.

To login:



1. Navigate to <https://portal.exostar.com>. Input your **Email Address** or **User ID**. Click **Next**.

2. Input your **Password**. Click **Next** to access the MAG Dashboard.

STEP 2: ACCESS TRADING PARTNER MANAGER (TPM)

Once you successfully login to your MAG account, ensure you authenticate with your credential. You can do this by selecting the Elevate Credential Strength button in the My 2FA Credentials section. The system also prompts for your credential once you select to access TPM.

To access TPM:

1. From the MAG Dashboard, select the **My Account** tab.
2. Select the **View Organization Details** sub-tab.
3. Click the **View in Trading Partner Management (TPM)** link.

The screenshot shows the Exostar user interface. At the top right, there is a 'Billing and Support' button. Below the logo, the user information is displayed: 'User : OSPatchingTest JanTwentyFiveTwentyTwentyThree(jantwentyfiveto_5023) | Organization : Jetty Full OS Patching Jan25 2023 | Credential Strength :'. A navigation bar contains 'Home', 'My Account', 'Administration', 'Registration Requests', and 'Reports'. Under 'My Account', there are links for 'Edit Profile', 'View Organization Details', 'Change Email', 'Change Password', 'Change Security Questions', 'Manage OTP', and 'Connect Accounts'. A notice asks if the user needs to change organization details and provides a link to a request form. Below this, the 'Organization Details' section is shown with fields for Organization Name, ID, Business Unit, and MPID, along with address and city information. The link 'View in Trading Partner Manager (TPM)' is highlighted with a red box.

4. The following screen displays. Review the notice. Click the **Continue** button to access the Organization's profile.

The screenshot shows a notice titled 'TO: Lockheed Martin Suppliers'. The text explains that in accordance with Government regulations, certain information about suppliers must be verified. It mentions the Small Business Act and the preference programs established pursuant to sections 8(a), 8(d), 9, or 15 of the Small Business Act. A 'Continue' button is highlighted with a red box at the bottom of the notice.

STEP 3: UPDATE CYBER SECURITY SECTION OF SELF CERTIFICATION

The CCRA Questionnaire provides questions related to the applicability of cyber Defense Federal Acquisition Regulation Supplement (DFARS) requirement and the handling of Sensitive Information, **which is required annually**. To update the Cyber Security section:



1. Select **Self-Certification** from the left-hand menu.

✔ Organization Summary
✔ Business Description
✔ Company Profile
✔ Socio-economic
✔ Self-certification
✔ History
✔ D&B Other Information
✔ Foreign (Non-U.S.) / Domestic (U.S.) Owned
✔ Payments/Remittance
✔ Contacts
✔ MAG Information
✔ TPA
Actions
Perform Recertification
Close

2. Scroll down to the **Cyber Security** section. **Review the information provided.**

Cyber Security
The purpose of this section is to allow for you to answer and certify to questions related to the applicability of cyber Defense Federal Acquisition Regulation Supplement (DFARS) requirement and the handling of Sensitive Information, which is required annually.
Instructions: 1. Read the questions on the applicability of cyber Defense Federal Acquisition Regulation Supplement (DFARS) and Sensitive Information and provide your answers. 2. Read the paragraph below beginning with the words 'By clicking...' then click the 'Submit Certifications and Representations' button. Then click 'Save' or 'Next' to proceed.
If you answered (1) or Yes to the following sections and completed the registration/recertification, you will receive instructions shortly via email on how to complete the required cyber security questionnaire. Completion of the registration process is required prior to completing the cyber security questionnaire. The information will be used as an input to manage risk. If you answered 2a, 2b, 2c, or No to the following sections, then no further information is required. You may proceed to the next section of the supplier profile.

3. Under the **Applicability of Cyber DFARS and NIST SP 800-171** section, review the question and select the applicable radio button for the answer.



IMPORTANT: Carefully review this section and select the appropriate answer.

If you select (1) Seller asserts that DFARS 252.204-7012 applies. (By so asserting, Seller is required to complete the Exostar Cybersecurity Compliance and Risk Assessment (CCRA) questionnaire and confirm assessment score in US DoD's Supplier Performance Risk System (SPRS).

Selecting options 2(a), 2(b), or (2c), asserting that DFARS 252.204-7012 and Covered Defense Information / Controlled Unclassified Information does not apply, will not prompt you to complete the CCRA questionnaire.

Applicability of Cyber DFARS and NIST SP 800-171

* Are you required to be compliant with the U.S. Defense Federal Acquisition Regulation Supplement ([DFARS 252.204-7012](#)) and associated National Institute of Standards and Technology (NIST) [NIST SP 800-171](#) ?

SELLER represents either that:

(1) Seller asserts that DFARS 252.204-7012 applies. (By so asserting, Seller is required to complete the Exostar Cybersecurity Compliance and Risk Assessment (CCRA) questionnaire and confirm assessment score in US DoD's Supplier Performance Risk System (SPRS).)

(2) SELLER asserts that it is exempt from DFARS 252.204-7012 for one of the following reasons (check one):

(a) None of the subcontracts received from LOCKHEED MARTIN contain DFARS 252.204-7012.

(b) The performance of SELLER's subcontracts with LOCKHEED MARTIN do not involve covered defense information as defined in DFARS 252.204-7012.

(c) All of the items offered to LOCKHEED MARTIN are commercial off-the-shelf items as defined in FAR 2.101.

For more information on the Onboarding Module (OBM) and the new Cybersecurity Compliance and Risk Assessment (CCRA), [click here](#).

On August 26, 2015, and updated December 30, 2015, the United States Department of Defense (DoD) issued a new interim rule making significant changes to the way the U.S. DoD addresses National Institute of Standards and Technology (NIST). As a supplier, you should be aware of the significantly expanded obligations for protecting unclassified Covered Defense Information (CDI) / Controlled Unclassified Information and related activities. Additional guidance related to the above DFAR clause and NIST document can be found at the links above.

[Click here to view or update the Cybersecurity Compliance and Risk Assessment \(CCRA\) questionnaire.](#)

- Under the **Handling Sensitive Information** section, the question will automatically be set to **Yes** if the **Applicability of Cyber DFARS and NIST SP 800-171** question is **(1)**. Otherwise, you need to assert whether you are receiving any **Sensitive Information** from Lockheed Martin.



NOTE: Once you answer both questions, you can begin the Cybersecurity Compliance Risk Assessment (CCRA) Questionnaire by selecting the highlighted link under either section.

Handling Sensitive Information

* Does your company receive Sensitive Information from Lockheed Martin? Yes No

For the purpose of this questionnaire, all references to "Sensitive Information" includes Proprietary Information, Third-Party Proprietary Information, Personal Information (PI), Personal Identifiable Information (PII), Export Controlled Information (ECI), and Controlled Unclassified Information (CUI) / Covered Defense Information (CDI).
If you are attesting that the cyber DFARS is applicable (above), then this answer should be Yes.

For more information on the Onboarding Module (OBM) and the new Cybersecurity Compliance and Risk Assessment (CCRA), click [here](#).

Click here to view or update the Cybersecurity Compliance and Risk Assessment (CCRA) questionnaire.

IMPORTANT: If you answer (1) on the DFARS applicability section or Yes to the handling Sensitive Information question, the CCRA form is automatically assigned to you.

5. Once all required sections are complete, click **Submit Certifications and Representations**.

By clicking "Submit Certifications and Representations" below, I *OSPatchingTest JanTwentyFiveTwentyTwentyThree* am authorized to attest to the accuracy of the representations and certifications contained herein, including certifying to the entire NAICS table. I understand that I may be subject to penalties if I misrepresent **Jetty Full OS Patching Jan25 2023** in any of the certifications to Lockheed Martin.

Clicking on the "Submit Certifications and Representations" button will save your selections and certify them for another year.

Submit Certifications and Representations

Certification Status	
Self Certification Status:	Current
Self Certification Date:	2023-12-05 16:31:42
Self Certification Expiration Date:	2024-12-04 16:31:42
Self Certification User ID:	jantwentyfiveto_5023@fis.evincibletest.com
Self Certification User Name:	OSPatchingTest JanTwentyFiveTwentyTwentyThree

NOTE: A confirmation message displays, and self-certification dates and user information displays below the message. The completed certification and representation are valid for one year from submission. The system sends your Organization Administrators annual expiration warning emails, starting 60 days in advance of the calculated expiration date. You can perform the certification and representation process at any time during the year.

STEP 4: COMPLETE THE CYBERSECURITY COMPLIANCE RISK ASSESSMENT (CCRA) QUESTIONNAIRE

Once you access OBM, the CCRA Questionnaire displays in the Pending Forms tab of the dashboard and displays important details for the form. To access and complete the CCRA Questionnaire:

1. Select the highlighted **Click here to view or update the Cybersecurity Compliance and Risk Assessment (CCRA) questionnaire** link to open the **Onboarding Module**.

NOTE: The link also displays under the **Handling Sensitive Information** section. OBM can also be accessed through the Managed Access Gateway (MAG) dashboard via the OBM tile.

Applicability of Cyber DFARS and NIST SP 800-171

* Are you required to be compliant with the U.S. Defense Federal Acquisition Regulation Supplement ([DFARS 252.204-7012](#)) and associated National Institute of Standards and Technology (NIST) [NIST SP 800-171](#) ?

SELLER represents either that:

- (1) Seller asserts that DFARS 252.204-7012 applies. (By so asserting, Seller is required to complete the Exostar Cybersecurity Compliance and Risk Assessment (CCRA) questionnaire and confirm assessment score in US DoD's Supplier Performance Risk System (SPRS).)
- (2) SELLER asserts that it is exempt from DFARS 252.204-7012 for one of the following reasons (check one):
 - (a) None of the subcontracts received from LOCKHEED MARTIN contain DFARS 252.204-7012.
 - (b) The performance of SELLER's subcontracts with LOCKHEED MARTIN do not involve covered defense information as defined in DFARS 252.204-7012.
 - (c) All of the items offered to LOCKHEED MARTIN are commercial off-the-shelf items as defined in FAR 2.101.

For more information on the Onboarding Module (OBM) and the new Cybersecurity Compliance and Risk Assessment (CCRA), [click here](#).

On August 26, 2015, and updated December 30, 2015, the United States Department of Defense (DoD) issued a new interim rule making significant changes to the way the U.S. DoD addresses National Institute of Standards and Technology (NIST). As a supplier, you should be aware of the significantly expanded obligations for protecting unclassified Covered Defense Information (CDI) / Controlled Unclassified Information and related activities. Additional guidance related to the above DFAR clause and NIST document can be found at the links above.

[Click here to view or update the Cybersecurity Compliance and Risk Assessment \(CCRA\) questionnaire.](#)

2. Locate the **CCRA Questionnaire** in the **Pending Forms** tab from the OBM Dashboard.

NOTES:

- Anyone with OBM access and that is assigned to the form, can update, or complete the questionnaire. The **Assigned To** section indicates the current user assigned to the form. **Only one person can be assigned to a form at any given time.**
- You can initiate work on the form only when the **Request Status** is at 40%.

IMPORTANT! If the Request Status is at 20%, it indicates either the form is not provisioned, or the invitee accepting the invitation and the designated organization administrator are two different users. In such cases, the designated organization administrator needs to re-assign the form to themselves. **See Step 3 below.**

- The **Form Progress** for a new form starts at 0% and the revision is 0.1 for a form that has never been started. In the provided screenshot, the user has already submitted the form

once and is now renewing it for the second time. Therefore, the Form Progress is at 100%, and the Revision is 1.1.

Pending Forms

CCRA Form - Exostar Demo

Request No: JFYNCFED

Initiated Date 12/05/2023
Due Date 01/19/2024
Assigned To [Shivani Admin](#)

Status New
Status Date 12/05/2023
Reassigned No

Revision 1.1
Form Progress 100%
Request Status 40%

1 - 1 of 1 items

3. Select the three dots action button located to the right. Select **Edit** from the menu.

NOTE: You can also reassign the form by selecting the three dots action button.

Pending Forms

CCRA Form - Exostar Demo

Request No: JFYNCFED

Initiated Date 12/05/2023
Due Date 01/19/2024
Assigned To [Shivani Admin](#)

Status New
Status Date 12/05/2023
Reassigned No

Revision 1.1
Form Progress 100%
Request Status

Edit
Reassign
Assign Approvers

NOTE: Alternatively, select the hyperlinked form name and choose **Edit Form** on the **Form Details** page. You also have the option to download the latest Excel file, accessible in the **Offline Form** section. This option requires you to complete the form offline and upload the CSV. Please review the instructions provided on the **Introduction** worksheet of the file.

Form Details CCRA FORM-form upload (test)

[Edit Form](#)

Recent Request

Request No	5PN4FVWY	Request Date	02/08/2024
Request Type	Assign (New)	Status Date	02/08/2024
Current Status	In Progress	Date Assigned	02/08/2024
Assigned To	srilakshmi bontu	Date Due	03/24/2024
Latest Revision	0.1	Requester's Name	Hemanth Kanugolu
Expires on	N/A	Requester's Email	Super_user_uat@6dxn1b09.mailosaur.net

Offline Form

[Download Editable CCRA Form \[xslm\]](#)

Upload Form [.csv]

[Browse...](#) No file selected.

IMPORTANT! If the **Edit** button is not displayed, the form is not currently assigned to you. Use the **Reassign** option to assign the form to the correct user. **Only one person can be assigned to a form at any given time.**

4. Review the **Introduction** page. Click **Next**.

CCRA FORM

Introduction

Instructions for Offline form

- FCI1
- CUI2
- SI5
- 6
- Submitter

Introduction

This Cybersecurity Compliance and Risk Assessment (CCRA) is developed by the Defense Industrial Base Sector Coordinating Council (DIB SCC) Supply Chain Task Force to drive a common set of cybersecurity requirements that both document compliance and measure risk. It's intended to reduce the burden on our suppliers, currently being assessed against multiple standards and in varied formats (often with overly complex and outdated cyber requirements).

The CCRA is built on a set of Scoping Questions that will dynamically add/remove questions from the survey based on the response provided. The Scoping Questions will identify the type of information (i.e., Federal Contract Information (FCI), Controlled Unclassified Information (CUI), Covered Defense Information (CDI), or other customer defined Sensitive Information), the supplier possesses, processes, transmits, and/or stores; and highlight other key risk factors such as when Information & Communication Technology (ICT) is being provided by the supplier. It will align them to a set of questions that will help us understand a supplier's compliance and risk posture.

Regulatory Compliance

Upon submission, you will be provided compliance status as described below:

- Valid Response
- Invalid Response
- Disabled/Non-editable Response
- Mandatory question to be answered

NOTE: Once the supplier begins working on the form, they have the flexibility to save the form and exit at any point. All entered information will be saved during this process.

CCRA FORM-form upload

Introduction

Instructions for Offline form

- FCI1
- FCI1a
- CUI2
- SI5
- 6
- 3.1.1
- 3.10.1

1. Does your organization receive 48 CFR 52.204-21, Basic Safeguarding of Covered Contractor Information, in the performance of US Federal contract(s)?

Yes

Guidance
Select Yes or No

If Scoping question 1 = Yes, user is presented with 1a and 6 FCI Cyber Security controls 3.1.1, 3.10.1, 3.13.1, 3.14.1, 3.14.2, 3.14.5.

See 48 CFR 52.204-21 for more details - <https://www.acquisition.gov/far/52.204-21>

- Valid Response
- Invalid Response
- Disabled/Non-editable Response
- Mandatory question to be answered

Exit Save Previous Next

5. Complete all questions in the form. Once you reach the last question, right before the **Submitter** page, you must select the **Submitter** option from the left-hand navigation to open the page. *There is no **Next** button.*

CCRA FORM-form upload

3.14.5 Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened or executed.

Yes

Guidance
Category 2
Select Yes only when the security control is fully implemented. Select No in all other cases; control is not implemented, partially implemented, or on POAM.
(ref., NIST SP 800-171 3.14.5 or CMMC SI.L1-3.14.5)

Periodic scans of organizational systems and real-time scans of files from external sources can detect malicious code. Malicious code can be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways including web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities.

Valid Response
Invalid Response
Disabled/Non-editable Response
Mandatory question to be answered

Please use the left navigation panel to continue to fill submitter details.

Exit Save Previous

6. Click the **Save** button.

IMPORTANT! Users must ensure they click the **Save** button prior to clicking the **SUBMIT** button at the end of the survey to complete the questionnaire. The **Save** button does not submit the survey for scoring or updates. The **Submit** button remains greyed out until ALL questions are answered and the form has been saved.

CCRA Supplier Demo

Introduction

Instructions for Offline form

FC1

CUI2

SI5

6

Submitter

Vendor Primary POC Name
Test

Vendor Primary POC Email
test@test.com

Vendor IT Security POC Name
Test

Vendor IT Security POC Email
test@test.com

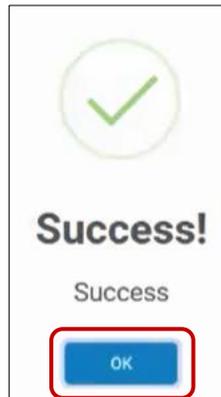
Vendor Local DUNS Number(s)
1234567

Vendor CAGE Code(s)
1234567

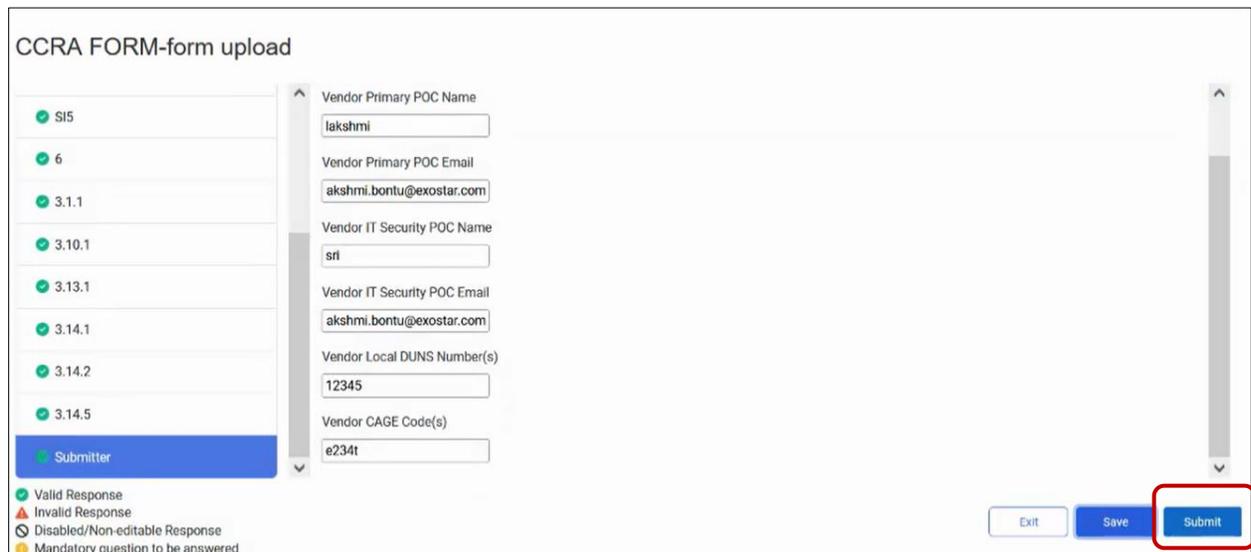
Valid Response
Invalid Response
Disabled/Non-editable Response
Mandatory question to be answered

Save Submit

7. Click **OK** to confirm save.



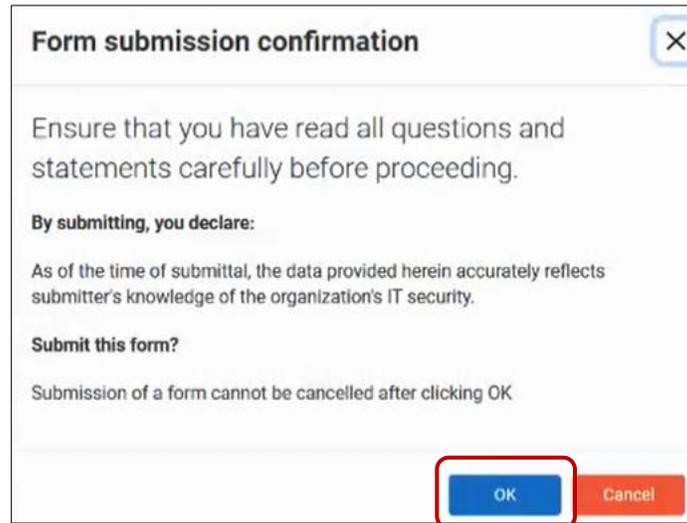
8. Click the **Submit** button.

The screenshot shows a web application interface titled "CCRA FORM-form upload". On the left side, there is a vertical list of items, each with a green checkmark icon and a label: "SI5", "6", "3.1.1", "3.10.1", "3.13.1", "3.14.1", "3.14.2", "3.14.5", and "Submitter". The "Submitter" item is highlighted with a blue background. Below this list is a legend with four items: a green checkmark for "Valid Response", a red triangle for "Invalid Response", a grey circle with a slash for "Disabled/Non-editable Response", and a yellow star for "Mandatory question to be answered". On the right side of the form, there are several input fields with labels: "Vendor Primary POC Name" (value: lakshmi), "Vendor Primary POC Email" (value: akshmi.bontu@exostar.com), "Vendor IT Security POC Name" (value: sri), "Vendor IT Security POC Email" (value: akshmi.bontu@exostar.com), "Vendor Local DUNS Number(s)" (value: 12345), and "Vendor CAGE Code(s)" (value: e234t). At the bottom right of the form, there are three buttons: "Exit", "Save", and "Submit". The "Submit" button is highlighted with a red rectangular border.

NOTE: Please see the [Submitter's Page Detail Guidance](#) section below for guidance on completing these fields.

IMPORTANT! If you complete the form offline and upload the completed form, you must complete this page directly in the Onboarding Module application online.

9. Click **OK** to confirm submission.



The image shows a 'Form submission confirmation' dialog box. It has a title bar with a close button (X) in the top right corner. The main text reads: 'Ensure that you have read all questions and statements carefully before proceeding.' Below this, it says 'By submitting, you declare:' followed by 'As of the time of submittal, the data provided herein accurately reflects submitter's knowledge of the organization's IT security.' Then it asks 'Submit this form?' and includes a warning: 'Submission of a form cannot be cancelled after clicking OK'. At the bottom, there are two buttons: a blue 'OK' button and a red 'Cancel' button. The 'OK' button is highlighted with a red rectangular box.

Please note as you progress through the form request, you will see the following **Request Status** percentages:

- **Pending Provisioning:** Request Status 20%
- **Provisioned:** Request Status 40%
- **First Time Access:** Request Status 60%
- **Form Started:** Request Status 80%

NOTES:

- Once the user submits the form, the form displays under the **Completed Forms** tab.
- The score summary details are displayed on the bottom right of the Forms Details page.
- **Recent Request** will be updated to include expiration date of the form.

- **Revision History** will display the latest revision. Additionally, you will have the ability to download all the revisions. The answers display along the right-hand side of the PDF.

The screenshot displays the 'Form Details' for a CCRA FORM upload (test). Key sections include:

- Recent Request:** Shows request details such as Request No (5PN4FVWY), Request Date (02/08/2024), Request Type (Assign (New)), Status Date (02/08/2024), Current Status (Completed), Date Assigned (02/08/2024), Assigned To (srilakshmi.bontu), Date Due (03/24/2024), Latest Revision (1.0), Requester's Name (Hemanth Kanugolu), Expires on (02/07/2025), and Requester's Email (Super_user_uat@6dm1b09.mallosaur.net).
- Revision History:** A table with columns for Revision, Type, SPRS Score, Date, and Download. It shows one revision (1.0, Submitted, NIA, 02/08/2024) with a download icon.
- Assignment History:** A table with columns for User and Date Assigned. It shows two assignments: Hemanth Kanugolu (02/08/2024) and srilakshmi.bontu (02/08/2024).
- Offline Form:** Options to download an editable CCRA Form (.xism) or upload a form (.csv).
- Compliance:** A section detailing compliance with various regulations (48 CFR 52.204-21, DFARS 252.204-7012, DFARS 252.204-7020, CMMC Certification Level) and risk assessments (Cyber Risk Rating, Risk of FCI-only suppliers).

Submitter's Details Page Guidance

Field Name	Guidance
Vendor Name	Company/Organization Name
Vendor Primary POC Name	First Name Last Name (i.e., John Doe)
Vendor Primary POC Email	Primary POC email address
Vendor IT Security POC Name	First Name Last Name (i.e., John Doe)
Vendor IT Security POC Email	IT Security POC email address
Vendor Local DUNS Number(s)	If more than one, use a comma and a space to separate values (i.e., 007505491, 000665432)
Vendor CAGE Code(s)	If more than one, use a comma and a space to separate values (i.e., 3T456, 56789)
If the response on this form is applicable to more than one of your organization's business units/divisions, provide all the Local DUNS Number and CAGE Codes that applies. You'll be able to export a single form for multiple DUNS/CAGE Code	

UPDATE COMPLETED FORM

To update the submitted form, you must renew the form. To do so:

1. Navigate to the **Completed Forms** tab.
2. Click **Renew** from the action button or from the **Forms Details** pages.

Pending Forms	Pending Approval Forms	Completed Forms	Cancelled Forms
CCRA Form - Exostar Demo Request No: JFYNCFED		Initiated Date 12/05/2023 Expiration Date 05/05/2024 Assigned To Shivani Admin	Form Status Completed Status Date 12/07/2023 Reassigned No
		Buyer Approval Status null Revision 2.0	Renew

NOTE: This action will move the form back to the **Pending Forms** tab.

3. Select to **Edit** the form and complete the steps as outlined above.

FORM UPGRADE

It is possible for your partner to upgrade a form from its previous version (i.e., add or remove questions). Once the form has been upgraded, you must edit the form and complete the upgraded questions. To upgrade a form:

1. Navigate to the desired **Form Details** page. Click the **Edit Form** button.

Form Details CCRA FORM-form upload (test)			
Edit Form			
Recent Request			
Request No	5PN4FVWY	Request Date	02/08/2024
Request Type	Assign (New)	Status Date	02/08/2024
Current Status	In Progress	Date Assigned	02/08/2024
Assigned To	srilakshmi bontu	Date Due	03/24/2024
Latest Revision	0.1	Requester's Name	Hemanth Kanugolu
Expires on	N/A	Requester's Email	Super_user_uat@6dxn1b09.mailosaur.net

2. An upgrade notification displays. Click the **Next** button.

Upgrade Form

This form has been recently revised and needs to be upgraded with your previously saved data in order for you to complete.
The upgrade will take a few minutes to finish, after which you can access the form again via the link to the form on the homepage.

Next

NOTE: The system can take up to five minutes to upgrade the form. You do not have to wait for form to upgrade and can **Exit** and come back later. If you do wait, a confirmation screen displays.



3. If you wait for the form to upgrade, click **Continue** from the confirmation screen to begin editing the upgraded form.



4. If you do not wait for the form to upgrade, you can **Exit** and come back later. Navigate to the **Form Details** page and click the **Edit Form** button to edit the upgraded form. Complete the form as you would normally.

FORM GROUPING

Form Grouping is used to share a completed form your organization filled out with your compatriot business units. The sections below provide step-by-step instructions on how to share your group form.

Business Issue

Company XYZ is composed of several subsidiary companies and/or business units (BU), each one of which is a Supplier to one or several Exostar Buyer organizations. Each of the subsidiaries is being asked to complete forms from one or more Buyer organizations. This results in requesting many of the subsidiaries to complete the same form. The security policies and infrastructure of the subsidiaries of Supplier XYZ are managed and controlled by a single shared service, an organizational unit located within one of the registered XYZ companies/subsidiaries. That unit can answer the form on behalf of many of the XYZ subsidiaries. This unit would like to answer the form once for all subsidiaries covered by its security program.



Solution

Exostar has the capability to create a Form Group of companies/businesses where one of the businesses can represent the group when completing forms. The XYZ business needs to nominate one of the business units as the source to represent the group. That business completes the form on behalf of the group (Destinations), and the results are provided to Buyers XYZ subsidiaries chose to share the results. In this way, the form is under the control of a single subsidiary or business unit within the group, but shared by any of the others with whatever Buyers they wish.

Destination organizations can share the group form with individual Buyers just like any other normal assigned form with two major exceptions:

- The form is locked and only the Source Organization can edit it. All further edits are reflected in the destination form in real-time.
- When a form is submitted, the scoring of the shared form applies to the one associated with Destination Organization as well.

Group Setup

Company XYZ needs to do the following to setup the group within Exostar:

1. Create a support case via the Support page and describe the case as Create a Form Group in OBM.
2. Provide the Form Grouping Submission Form that identifies:
 - a. The source business unit by its Exostar ID, DUNS ID, full address, and email address of the responsible person who will handle the security form.
 - b. The destinations or business units within the group by Exostar ID, DUNS ID, and address for each.
 - c. Which form is to be shared with the Destinations.
3. Exostar contacts each destination business unit to confirm they will be added to the new group.
4. Exostar creates the group within the organization data and the form from the source will be available for the destinations.

NOTES:

- The source organization must submit the form for the responses to be duplicated onto their respective destination organization forms.
- If a new supplier is added to the existing Form group, the Source organization must resubmit (renew) the form for the responses to be duplicated onto their respective destination organization forms.

View Form Groups

Suppliers can determine if their form groups have been migrated to the Buyer's OBM application by going to the specific form in the Buyer's OBM and reviewing the Form Details page to determine if they are a destination of a form group. The message will read: **This form is being shared by the following organization ORGNAME. You do not have permissions to edit this form.**

The screenshot below shows the form is provided by another organization, which is the **Source** of the completed form.

Form Details CCRA FORM (CCRA Questionnaire)

[View](#)

This form is being shared by the following organization :New_Supplier_SEM_One (115340730). You do not have permissions to edit this form

Offline Form

[Download Editable CCRA Form\(.xlsx\)](#)
Upload is enabled to only active status

Recent Request

Request No	5CJKTST	Request Date	02/29/2024
Request Type	Assign (New)	Status Date	03/05/2024
Current Status	New	Date Assigned	02/29/2024
Assigned To	Suboah Achapea	Date Due	04/14/2024
Latest Revision	-	Requester's Name	Heimanth Kanugolu
Expires on	N/A	Requester's Email	Super_user_uat@6dxn1b09.mailosaur.net

Revision History

Revision	Type	SPRS Score	Date	Download
----------	------	------------	------	----------

CCRA FORM has not yet been submitted.

ONBOARDING MODULE RESOURCES

The following OBM resources are located on Exostar's Self-Help portal:

- [Onboarding Module](#): This landing page provides an application overview, roles and responsibilities, as well as additional resources links.
- [Onboarding Module Get Started](#): This page provides access instructions.
- [Onboarding Module Training Resources](#): This page provides downloadable guides for Buyers, Suppliers, and Reporting.