Update Your Organization

Follow the steps below to update your organization’s cybersecurity posture within Trading Partner Management (TPM) and Partner Information Manager (PIM).

**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 go to [http://myexostar.com/lm2fa/](http://myexostar.com/lm2fa/).

**Note:** There must be at least one active LMP2P user (including the Organization Administrator), with 2FA credentials associated with the organization, in order to recertify an organization.

Access

Follow the steps below to login to access Trading Partner Manager (TPM):

1. Login to Exostar Managed Access Gateway (MAG) at [https://portal.exostar.com](https://portal.exostar.com). For help with resetting your MAG password or if you forgot your login credential, refer to the [MAG User Guide](https://portal.exostar.com).

   **Note:** If you are the first user in your organization to access PIM, you need to accept the standard MAG Usage Service Agreement. If you see View Service Agreement on the Partner Information Manager row in your MAG account, click the link and accept the service agreement.

2. Click the **My Account** tab and then click the **View Organization Details** sub-tab. Click the View in Trading Partner Management (TPM) link.
3. Review the notice and click **Continue** to access your organization’s TPM profile.

4. Select the **Cybersecurity** option from the left-hand menu.

5. Update Cybersecurity and DFARS/NIST Questionnaires (if applicable).

**Important**: Cybersecurity is important to Lockheed Martin, and the questionnaire has been implemented to mitigate risks to suppliers as it relates to sensitive information.

- If your company receives and processes sensitive information from a third-party company (e.g. one of the Exostar partners such as Lockheed Martin), you must click the **YES** button.
- If your company is required to be compliant with the US Defense Acquisition Regulation Supplement (**DFARS 252.204-7012**), and associated **NIST SP 800-171** you must click the **YES** button.
- If you answered **YES** to either question, you are required to complete the applicable questionnaire(s). Questionnaires are hosted in Exostar’s Partner Information Manager
(PIM) application. Clicking the links within TPM (see below) give you access to the questionnaires.

**Note:** The Cybersecurity Questionnaire serves as an indicator of supplier cyber maturity or to highlight the need to mitigate risks of sharing LM Sensitive Information. The NIST SP 800-171 Questionnaire answers the DFARS 252.204-7012 required cybersecurity self-assessment for suppliers who process, store, or transmit Covered Defense Information.

![Cyber Security Questionnaire](image)
![NIST Questionnaire](image)

6. Access the Cybersecurity Questionnaire or the NIST SP 800-171 Questionnaire.

Please refer to the [Partner Information Manager Supplier Guide](#) for information on PIM and filling out questionnaires.