Cybersecurity – Supplier's Frequently Asked Questions

Table of Contents

Cybersecurity – Supplier's Frequently Asked Questions

Cybersecurity – Supplier's Frequently Asked Questions

General Questions:

1. **How many questionnaires are there, and which am I required to complete?**

There are two questionnaires; Cybersecurity Questionnaire and the NIST SP 800-171R1.

- **Cybersecurity Questionnaire (CSQ):** The one hundred ninety-four (194) cybersecurity questionnaire developed by Exostar Partners (Lockheed Martin, Boeing, Northrup Grumman, BAE systems, and Raytheon) hosted on Exostar's Partner Information Manager (PIM). This set of questions is based on the Center for Internet Security Critical Security Controls. (CSC). The purpose of the Cybersecurity Questionnaire is to measure a company's current cyber security capability and help you understand potential actionable steps as well as industry security best practices to improve your cyber security posture. Reference the Exostar Process FAQ for Suppliers.

  Lockheed Martin requires cybersecurity self-assessments for those suppliers of services or products with which Lockheed Martin **shares sensitive information**. Sensitive information is defined by LM as information in any or all the following categories:

  1. Personal Information (PI)
  2. Export Controlled Information (ECI)
  3. Lockheed Martin Proprietary Information (LMPI)
  4. Third Party Proprietary Information (TPPI)

  Generally, if a Non-Disclosure Agreement (NDA) or Proprietary Information Agreement (PIA) is executed between LM and the vendor, then sensitive information is shared, and the vendor would be required to complete, at the minimum, the Cybersecurity Questionnaire.

  Please see the *Trading Partner Manager Profile Sensitive Information Checklist* section of the Lockheed Martin Supplier Cybersecurity webpage for additional information.

- **NIST SP 800-171 Questionnaire (NIST):** Also referred to as the DFARS/NIST Questionnaire. This set of one hundred-nine (110) questions directly addresses compliance to the requirement outlined in the NIST SP 800-171 standard mandated by DFARS 252.204-7012. This tool can be used to help identify deficiencies against the NIST SP 800-171 requirements.

  The NIST questionnaire is required for those suppliers for which Lockheed Martin flows down DFARS Clause 252.204-7012 and where Covered Defense Information is or will be shared. Covered Defense Information is defined as follows:

  "Covered defense information" means unclassified *controlled technical information* or other information, as described in the Controlled Unclassified Information (CUI) Registry at https://www.archives.gov/cui/registry/category-list.html

  (1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

  (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

Cybersecurity – Supplier's Frequently Asked Questions

Examples of CDI Markings:

a. Distribution B: US Govt. Only
b. Distribution C: US Govt. & Contractors
c. Distribution D: DoD & US DoD Contractors
d. Distribution E: DoD only
e. Distribution F: Further dissemination only as directed by controlling office
f. DoD Export Controlled markings

Please see the *Trading Partner Manager Profile Sensitive Information Checklist* section of the Lockheed Martin Supplier Cybersecurity webpage for additional information.

2. **What expertise is needed to understand how to improve my company's cybersecurity posture.** Understanding and improving cyber capability level requires knowledgeable IT and Cyber talent. If the supplier does not have such skills, engaging local IT support companies or outsourcing the IT and Cyber functions should be considered to improve a company's capability level. Potential criteria for selecting an appropriately qualified support company may include, but not be limited to, ensuring the company's cyber talent have generally accepted industry certifications. Guidance on appropriate level of cybersecurity credentials can be found throughout many sources. Two sources are provided for ease of reference. The supplier is encouraged to investigate the full range of sources of cybersecurity credentials.
   1. National Initiative for Cybersecurity Careers and Studies (NICCS). This site provides a comparison of the major cybersecurity certifications.
   2. US Department of Defense (DOD) 8570.01-M provides guidance on various baseline cyber certifications. A baseline certification must be obtained by any supplier members supporting the DoD who have privileged system access performing IA functions (i.e., Information Assurance Technical) or who provide design functions such as Information Assurance System Architecture and Engineering (IASAE).
      a. In addition to the IA baseline certification requirement for their level, IATs or IASAEs who also perform IAT functions must successfully pass the appropriate CE training course (for example a Cisco OS or Linux+ OS training course test). The CE certificate must be obtained through industry vendor-provided training. FedVTE training and other commercial training courses are excellent training venues, but they do not satisfy the requirement for the vendor OS CE baseline certificates.

Cybersecurity – Supplier's Frequently Asked Questions

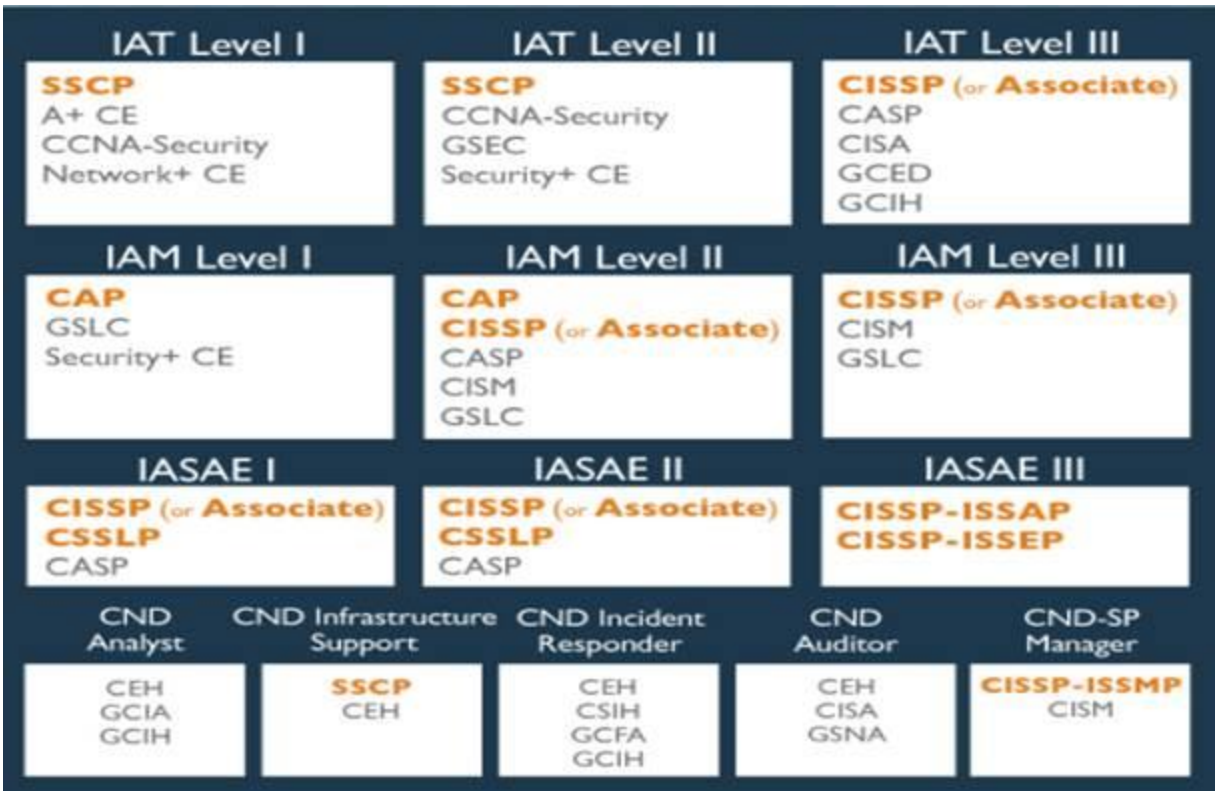


Figure Q2 DoD Directive 8570.1 Cyber Certifications Guidance

With any decision to engage an external company, the supplier should evaluate the company's reputation, work product and performance among other business requirements.

For information about why Lockheed Martin is requiring completion of the new cyber questionnaires, or information on Lockheed Martin's general supply chain cybersecurity strategy refer the Lockheed Martin corporate website and the suppliers link at the top right www.lockheedmartin.com/us/suppliers/cyber-security.html.

3. What are the Capability Levels (Cybersecurity Questionnaire) and what do they mean?

Capabilities Levels are derived based on the supplier's response and submission of the Cybersecurity Questionnaire.

There are five capability levels. They are an indicator of a supplier's ability to guard against cyber-attacks. A higher cybersecurity capability directly corelates with the ability to protect sensitive information. It potentially engenders confidence and may create competitive advantage. In contrast, a lower cybersecurity capability could raise questions regarding a supplier's ability to adequately protect sensitive information and may require more risk mitigations. The capability levels are defined as follows:

Level 0	No or minimal cyber risk management program; significant cyber protections are lacking; additional risk mitigations must be implemented
Level 1	Basic level cyber risk management program; some protections in place but additional risk mitigations must be implemented

Cybersecurity – Supplier's Frequently Asked Questions

Level 2	Moderate level cyber risk management program; good protections in place but additional risk mitigations are required to protect sensitive information
Level 3	Solid performing cyber risk management program; strong protections have been implemented; advanced threats are understood and taking steps to address with specific controls; additional risk mitigations are likely needed to protect against advanced risk
Level 4	Cyber risk management program that can detect, protect against, and respond to advanced threats; specific advanced controls are implemented
Level 5	Cyber risk management program that can detect, protect against, and respond to advanced threats; specific advanced controls are implemented and optimized on an ongoing basis

4. How can a supplier improve their Capability Level score?

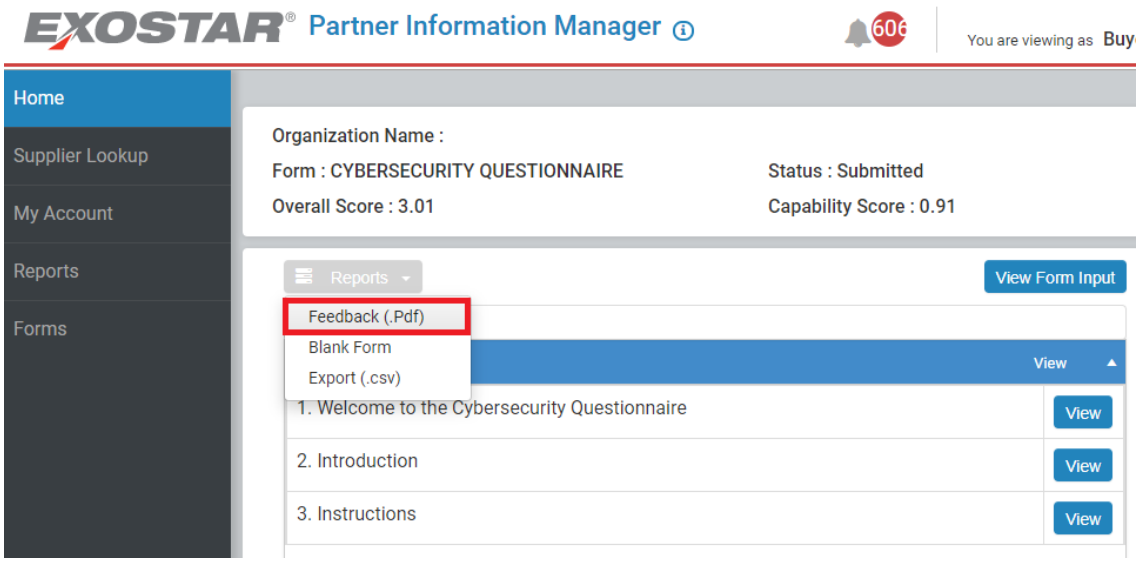
Lockheed Martin first recommends that the supplier fully understands three documents that are available on the Exostar Partner Information Manager (PIM) Cybersecurity Questionnaire site

a. Control Activity to Capability Level Matrix
   1) Provides a listing of all controls on the Cybersecurity questionnaire relative to their Capability Levels. Use this to identify which controls are required to be implemented to achieve a Green rating.

b. Process FAQ For Suppliers – Frequently asked questions about the completing the Exostar questionnaires

c. Exostar Cybersecurity Questionnaire Feedback Report (PDF) – Upon completion of the questionnaire, Exostar provides a feedback report within the Partner Information Manager (PIM) system. The report provides details on how the scoring and ratings are calculated along with actions on how to improve their cybersecurity ratings. Screenshot on where the report can be obtained is provided below.

This resource provides instructions on how to complete the questionnaire and obtain the feedback report – Partner Information Manger Supplier Guide



Cybersecurity – Supplier's Frequently Asked Questions

5. What are the Cyber Ratings and how can suppliers reach the desired "Green" rating?

Lockheed Martin's goal is to drive our critical suppliers to a capability Level 3 (Green Rating) or higher on the cybersecurity questionnaire. Achieving a Level 3 requires that the supplier implements all the controls for Level 1, Level 2, and Level 3 on the Cybersecurity Questionnaire.

Upon completion of the Cybersecurity Questionnaire, the supplier is provided with a Feedback report within Exostar Partner Information Manager (PIM). This report provides details on how the scoring works and what control the supplier needs to implement to achieve a Capability Level 3 – which corresponds internally to a Cyber rating of Green. See previous FAQ for information on how to obtain a feedback report from Exostar.

6. I've completed the NIST Questionnaire per DFARS 252.204-7012, but I am not shown as compliant. What do I need to do to become compliant?

The Exostar NIST questionnaire now provides four different response options. For each control suppliers may select one of the following:

a. **Implemented:** Implemented per the NIST 800-171 R1 specification
b. **Addressed with System Security Plan (SSP) & Plan of Actions and Milestones (POAM):** You have documented in an SSP & POAM how you will become compliant with the control.
c. **Approved Exception:** You have been given approval by the DoD to: (1) treat this control as not applicable or (2) provide an equally effective alternate control.
d. **Not Implemented:** The control has not been implemented, nor is there any plan to implement it as part of an SSP & POAM. (*This response does not comply with DoD requirements.)*

Where appropriate, for unimplemented controls you may now update your submittal as: (b) **Addressed with SSP & POAM** or (c) **Approved Exception.** These responses, in addition to the controls that your company has identified as implemented, support our understanding of your company's ability to demonstrate compliance to the NIST Questionnaire.

7. Can we get an electronic (PDF) version of the questionnaires?

The links to the PDF version of the questionnaire is provided below. Please note that the only acceptable form of submission for this requirement is electronically through Exostar's Partner Information Manager (PIM) portal.

- Blank Cybersecurity Questionnaire – Download
- Blank NIST SP 800-171 - Download

8. What resources are available to help a supplier with implementing the NIST controls?

NIST 800-171 Control Guidance

- NIST Special Publication **800-171** Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- NIST Special Publication **800-171A** Assessing Security Requirements for Controlled Unclassified Information
- NIST Special Publication **HB 162** NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements

Cybersecurity – Supplier's Frequently Asked Questions

Documentation Templates

- Example of an *SSP* (**System Security Plan template**) (.docx)
- Example of a basic *POA&M* (**Plan-of-Action-and Milestones template**) (.docx)

Links for *CUI* (Controlled Unclassified Information)

- **CUI Registry**
- Enumerated list of **CUI categories**
- **CUI marking handbook** (.pdf)
- **CFR Title 32 Vol 6 Sec 2002-20** (.pdf)

DoD Cyber **Incident Reporting** for contractors and subcontractors

9. What resources are available to help a supplier with implementing the controls on the Cybersecurity Questionnaire.

Cyber Security Questionnaire resources:

- **Controls Guidance** (.pdf)
- Cyber Security Controls Questionnaire process **FAQ** (.pdf)

10. I am a provider of consulting services and/or labor resources. Am I required to complete the questionnaires?

Within services contracts, such as consulting services or experienced non-Lockheed Martin labor resources, it is generally assumed that Lockheed Martin Sensitive Information is shared. It can be further assumed that if there is an executed Non-Disclosure Agreement (NDA) or similar legal construct then Sensitive Information is shared. If the supplier's employees process, store and or transmit such sensitive information exclusively using Lockheed Martin's IT assets then the cybersecurity self-assessments are not required. If the supplier's employees process, store and or transmit such sensitive information using *any of* the supplier's IT assets then the cybersecurity self-assessments *must be completed* and minimally it is expected that the supplier completes the first questionnaire (sensitive information) and if DFARS is applicable the NIST 800-171 questionnaire. Questions as to specifics about information shared by Lockheed Martin and your company should be addressed directly with your Lockheed Martin primary engagement interface.

11. We currently do not hold any contracts with LM, do we still have to complete this requirement?

If you have in the past, currently, or will in the future; store, process or transmit Lockheed Martin Sensitive Information you are required to complete the questionnaires regardless of holding contracts with Lockheed.

Lockheed Martin will use the response to these surveys as a basis of evaluation for future supplier selections and contract commitments.

Cybersecurity – Supplier's Frequently Asked Questions

Reminder notices from Exostar and Lockheed Martin

12. Why do I keep receiving follow up/reminder emails from Lockheed Martin and Exostar?

If you are receiving follow up emails after completing the questionnaires, then review of our records indicated that you have not satisfied all the cybersecurity requirements. Please review your Trading Partner Manager (TPM) vendor profile and Partner Information Manager (PIM) accounts to ensure that all questions have been properly updated, saved, and submitted.

Please use the TPM-PIM-User Guide.pdf (User Guide) with the following review steps:

Trading Partner Manager Review:

Step 1: Log into TPM and navigate to the Cybersecurity page (User Guide Step 1 -4)
Step 2: Review Update "Handing Sensitive" information. (User Guide Step 5)
Step 3: **Ensure that the NIST/DFARS questions is not blank or null.** (User Guide Step 5)
Step 4: Save and update your response.

Partner Information Manager Review:

Step 1: Complete Step 1 through Step 4 from above.
Step 2: Click on either "Click here to view Cyber security questionnaire" or "Click here to view NIST SP 800-171 Questionnaire" to be linked to the PIM Dashboard. (see PIM Supplier Guide.pdf)
Step 3: Click on the **Forms Summary** Widget and select either the Cybersecurity or NIST Questionnaire.
Step 4: Ensure that you go to the end of each questionnaire and click on the "***Submit Response***" button to save and submit the questionnaire for scoring.
Step 5: See PIM Supplier Guide.pdf for instructions on how to complete the questionnaire

13. I've already completed the questionnaires, but I am still receiving reminder notices.

In addition to completing the questionnaires, suppliers are required to keep questionnaires current (updated within the last 12 months). Upon receipt of reminder notices the supplier must log back into Exostar, make updates to their questionnaires, and re-submit the questionnaire to complete this requirement.

For instructions on how to update/complete the questionnaire, please use the *PIM Supplier Guide* from the Exostar's Downloadable Guides - PIM page.

Replication: Form Groups

14. We have more than one business unit that are suppliers to Lockheed Martin with accounts in Exostar, do we have to manually complete the questionnaires for each account?

No, Exostar's Form Group function have been developed to allow organizations to share a completed Cybersecurity and/or NIST questionnaire across multiple business units. Lockheed Martin requires that companies with multiple entities must manage IT and cybersecurity centrally across all eligible entities. Furthermore, all eligible related entities must be governed by the same centralized IT and cybersecurity policies. If your company meets those eligibility requirements then your company can be configured for From Grouping.

Cybersecurity – Supplier's Frequently Asked Questions

The process for requesting Form Group is provided here: https://exostar.atlassian.net/wiki/display/SEC/Form+Groups:+using+forms+completed+by+other+BUs

The completed spreadsheet should be submitted to Exostar Online Support.

15. **I've already completed the Form Group request for my organization's account but need to add or remove accounts from this form group because they are no longer part of our organization.**

To add accounts to an existing form group, you must complete the form group request using the same master account previously used and just the additional accounts you need to the destination account fields. Once complete, submit the new request to Exostar Online Support.

To remove account(s) from an existing form group, please contact Exostar Online Support

TPM related questions:

16. **How do I get to the TPM portal?**

Suppliers can access the TPM portal by following Step 1 through 4 of the TPM-PIM-User Guide.pdf (User Guide).

17. **I've answered "Yes" to both the Cybersecurity Questionnaire and NIST Questionnaire, but I am still unable to access PIM to complete the questionnaires.**

Please contact Exostar Online Support

PIM Related Questions:

18. **How can I access and complete the Cybersecurity questionnaire?**

Suppliers can gain access to the questionnaires by following the instructions below:

a. Log in to TPM portal and update your Cybersecurity profile. (Step 1 through 4 : TPM-PIM-User Guide.pdf)
    1) Click on the hyperlink "**Click here to view the cyber security questionnaire**" to assign and complete the new questionnaire.

b. Please answer the question concerning the NIST SP 800-171. If you are required to be compliant with DFARS 252.204-7012, then the answer to this question will be "Yes." If not, please select "No"
    1) If you've answered "Yes," you will be provided with a Hyperlink, "**Click here to view the NIST SP 800-171 questionnaire**" to assign and complete the questionnaire on Exostar's PIM system.
    2) If you've answered "No," no further action for the NIST SP 800-171 questionnaire is required.

c. Once you've logged into the PIM portal, please use the *PIM Supplier Guide* from the Exostar's Downloadable Guides - PIM page for detailed instructions on how to complete/update the questionnaires.

19. I can see the Questionnaire(s) on the PIM dashboard, but how can I start responding?

To complete the questionnaire you must **assign** the questionnaire to the appropriate personnel responsible for completing it.

- Instructions to **assign** the questionnaire is provided in the PIM Supplier Guide.pdf (User Guide).

20. I am in PIM, but I do not see any questionnaires available for completion.

Please follow the guidelines below while referencing the TPM-PIM-User Guide.pdf (User Guide).

Validate if you have responded to the handling sensitive information and NIST/DFAR question on your cybersecurity portion of your TPM vendor profile. (User Guide Step 1 through 5)

a. If both responses are "No," then you have acknowledged that you are not handling Lockheed Martin sensitive information and not required to be NIST/DFAR compliant. You are not required to complete neither the NIST nor CSQ questionnaire(s).
b. If one or both is "Yes," then click on:
    i. **Click here to view the Cybersecurity Questionnaire** – to access the Cybersecurity questionnaire, or
    ii. **Click here to view the NIST SP 800-171 Questionnaire** – to access the NIST questionnaire.
c. If you are still unable to see the questionnaire(s) on your PIM Dashboard, please contact Exostar Helpdesk online at http://myexostar.com/Online-Support/

21. I've completed the questionnaires but my LM Buyer/Subcontract Administrator says that it is not completed on their systems.

Ensure that the supplier has clicked on the "Submit Response" button at the end of the questionnaires. This will submit the questionnaire for scoring and push updates to integrated systems.

This resource provides instructions on how to complete the questionnaire – Partner Information Manger Supplier Guide: https://my.exostar.com/display/TE/Downloadable+Guides+-+PIM?preview=/32016800/32017214/PIM%20Supplier%20Guide.pdf

Screenshot of "Submit Response" button located only at the end of each questionnaire:

Cybersecurity – Supplier's Frequently Asked Questions